

Dedicated to Global First Responders

CBRNE

NEWSLETTER



October 2017



www.cbne-terrorism-newsletter.com

IOI
International
CBRNE
INSTITUTE



DIRTY R-NEWS

How Trump Can Destroy Kim Jong Un's Nukes Without Blowing Up the World

Source: <http://www.newsweek.com/donald-trump-north-korea-kim-jong-un-nuclear-nukes-missiles-669308>

Sept 23 – In the long view of history, North Korea getting a nuclear-tipped intercontinental missile in 2017 is the rough equivalent of an army showing up for World War II riding horses and shooting muskets.

Nukes are so last century. War is changing, driven by cyberweapons, artificial intelligence (AI) and robots. Weapons of mass destruction are dumb, soon to be whipped by smart weapons of pinpoint disruption—which nations can use without risking annihilation of the human race.

If the U.S. is innovative and forward-thinking, it can develop technology that ensures no ill-behaving government could ever get a nuke off the ground. Then we might be able to relax and return to laughing at Kim Jong Un for looking like the Stay Puft Marshmallow [Man topped](#) by a small furry mammal.

This is the argument in a new [book](#), *Striking Power: How Cyber, Robots, and Space Weapons Change the Rules of War*, by international law professors John Yoo (University of California, Berkeley) and Jeremy Rabkin (George Mason University). Their book connects war and nuclear weapons to a profound shift in the way the world works. We're moving away from an era of mass production, mass media and mass markets, and into an era when products, media, markets and everything else are hyper-targeted and highly personalized. I've been researching that broad shift for a book that comes out in March, and it makes sense that it applies to war too.

Economics of the 20th century were all about the masses. To be successful, a factory would strive to make the same product for the most people. TV networks sought to air least-common-denominator shows that would appeal to the broadest audience. In such a milieu, bigger usually won. Economies of scale ruled, "so we saw huge armies with identical mass-produced weapons that were cheap to make and caused a lot of indiscriminate destruction," Yoo tells me.

World War I was the first mass-market war, as reflected in its grim statistics: the Allies lost 5 million killed, 12.8 million wounded; the Central

Powers lost 8.5 million killed, 21 million wounded. "Efficiency did not stop with the production of consumer goods," Yoo and Rabkin write. "It extended even to the business of killing." Nuclear weapons multiplied those economies of scale—the goal was to make one big weapon that could wipe out whole cities. Nobody ever built a more efficient mass-market killing machine.

These days, that mentality is morphing. Think about the way Facebook, Google and Amazon use AI to learn about you and effectively market directly to you. You're becoming more of a market of one instead of a plebe in the mass market. The more technology can customize products, the more we'll demand products built just for each of us, not mass-produced stuff made for everybody.

In the military, this hyper-targeting is exactly what drones are about. Instead of leveling a village, as the U.S. did in Vietnam ([watch Ken Burns's new series](#)), we would build one robotic flying machine to seek out and kill a targeted individual. As Yoo and Rabkin point out, the Obama administration deployed a software virus called [Stuxnet](#) in 2010 to disrupt Iran's nuclear weapons program but do no other damage. "Cyberweapons have this precision effect, and they don't destroy anything or kill anyone," Yoo says.

Last year, Russia taught us a lesson in new-century warfare, if you can even call it warfare. Multiple intelligence agencies have concluded that Russia essentially achieved regime change in the U.S. by relying on narrowly directed hacks and hyper-targeted influence campaigns, like those fake ads that [Facebook](#) recently revealed. After nearly 70 years of pointing nukes at the U.S., Russia just had its most disruptive impact on it with nothing but computer code.

All of this suggests an approach to North Korea that has little in common with [threatening](#) "fire and fury like the world has never seen," as President Donald Trump so quaintly put it. He'd have been barely less in sync with the times if he'd promised to make it rain for 40 days and 40 nights.



Instead, Yoo suggests, the U.S. should go on the offense with cyberweapons designed to do things like make missiles malfunction (which maybe it has already [done](#), but *shh!*), erase data from military computers, wipe out the country's bank accounts or even steal and publicize Kim's smoochy emails to Dennis Rodman. It might send out tiny, barely detectable, AI-driven drones that work together like swarms of bees to take out key assets or people. In the longer run, Yoo says, it's feasible to develop satellite-based anti-missile technology armed with AI that could watch other nations, learn what an impending missile launch looks like and immediately fry the thing with lasers.

This isn't to say robot and software weapons are not dangerous to the world. They could do enormous damage and lead to many deaths if they disrupt the systems—power, water, food, communications—that keep societies going. Something like the mutually assured destruction

deterrent of the nuke era must emerge—a knowledge that retaliation in kind is likely, so everybody better cyber-behave. You might call it a new code war. At least it seems less terrifying than wondering if a nutjob is going to lob an atomic missile into Beverly Hills.

If the U.S. plays it smart, it will move out of the atomic age of war and into the AI age of war, and render Kim's nuclear ambitions meaningless. Of course, that would require leadership from a tech-savvy, innovative and forward-thinking American president—so...oops.

"New technology gives countries more options than just the tragic choice of either let this madman have a nuclear arsenal or trigger a conventional war," Yoo says. Ultimately, we'd like to be able to say to Kim or any nuke-seeking leader: Yeah, go ahead and build that useless weapon. What are you going to do next, develop a crossbow?

What Is the Difference Between a Hydrogen Bomb and an Atomic Bomb?

Source: <http://time.com/4954082/hydrogen-bomb-atomic-bomb/>

Sept 22 – North Korea warned this week that it might test a hydrogen bomb in the Pacific Ocean, after saying the country had already successfully detonated one.

A hydrogen bomb has never been used in battle by any country, but experts say it has the power to wipe out entire cities and kill significantly more people than the already powerful atomic bomb, which the U.S. dropped in Japan during World War II, killing tens of thousands of people.

As global tensions continue to rise over North Korea's nuclear weapons program, here's what to know about atomic and hydrogen bombs:

Why is a hydrogen bomb stronger than an atomic bomb?

More than 200,000 people died in Japan after the U.S. dropped the world's first atomic bomb on Hiroshima and then another one three days later in Nagasaki during World War II in 1945, according to the Associated Press. The bombings in the two cities were so devastating, they forced Japan to surrender. But a hydrogen bomb has the potential to be 1,000 times more powerful than an atomic bomb, according to several nuclear experts. The U.S. witnessed the magnitude of a hydrogen bomb when it tested one within the country in 1954, the *New York Times* reported.

Hydrogen bombs cause a bigger explosion, which means the shock waves, blast, heat and radiation all have larger reach than an atomic bomb, according to Edward Morse, a professor of nuclear engineering at University of California, Berkeley.

Although no other country has used such a weapon of mass destruction since World War II, experts say it would be even more catastrophic if a hydrogen bomb were to be dropped instead of an atomic one.

"With the [atomic] bomb we dropped in Nagasaki, it killed everybody within a mile radius," Morse told *TIME* on Friday, adding that a hydrogen bomb's reach would be closer to 5 or 10 miles. "In other words, you kill more people," he said.

Hall, director of the University of Tennessee's Institute for Nuclear Security, called the hydrogen bomb a "city killer" that would probably annihilate between 100 and 1,000 times more people than an atomic bomb.

"It will basically wipe out any of modern cities," Hall said. "A regular atomic bomb would still be devastating, but it would not do nearly as much damage as an H-bomb."

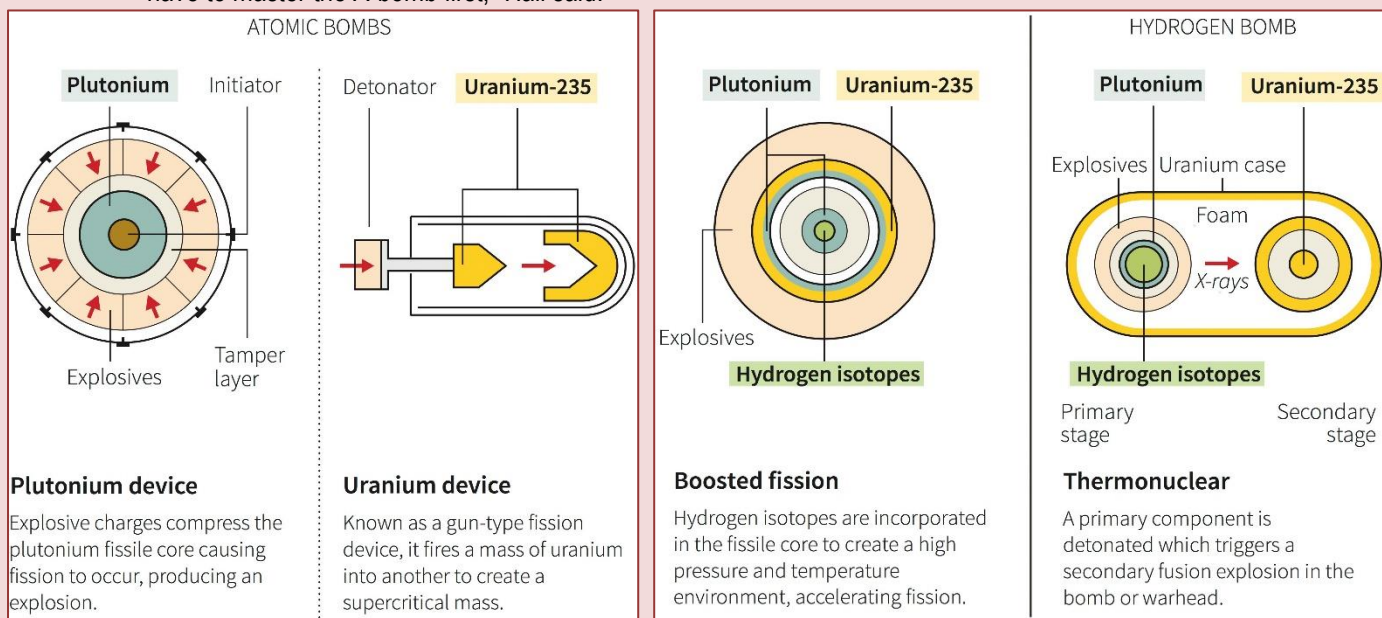




Hiroshima in ruins following the atomic bomb blast. Bernard Hoffman—The LIFE Picture Collection/Getty Images

What's the difference between hydrogen bombs and atomic bombs?

Simply speaking, experts say a hydrogen bomb is the more advanced version of an atomic bomb. "You have to master the A-bomb first," Hall said.



An atomic bomb uses either uranium or plutonium and relies on fission, a nuclear reaction in which a nucleus or an atom breaks apart into two pieces. To make a hydrogen bomb, one would still need uranium or plutonium as well as two other isotopes of hydrogen, called deuterium and tritium. The hydrogen bomb relies on fusion, the process of taking two separate atoms and putting them together to form a third atom.

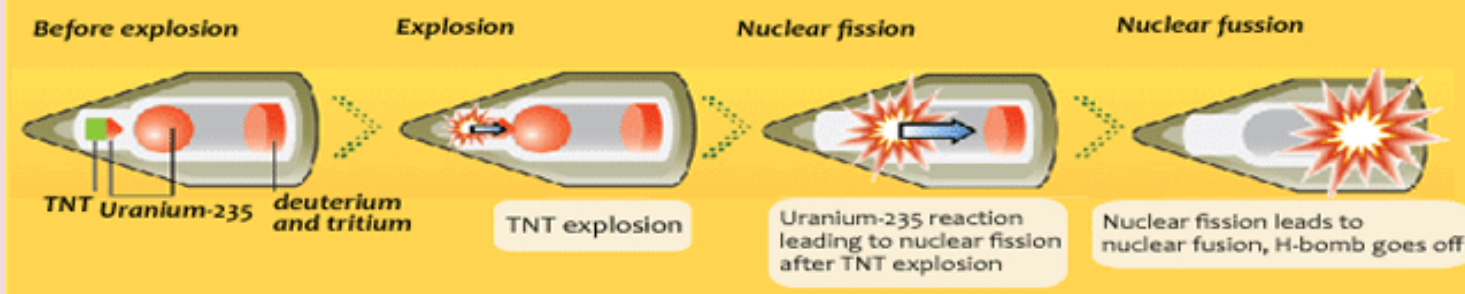
"The way the hydrogen bomb works — it's really a combination of fission and fusion together," said Eric Norman, who also teaches nuclear engineering at UC Berkeley.



Working Principle of Atomic Bomb



Working Principle of Hydrogen Bomb



In both cases, a significant amount of energy is released, which drives the explosion, experts say. However, more energy is released during the fusion process, which causes a bigger blast. "The extra yield is going to give you more bang," Morse said.

Morse said the atomic bombs dropped on Japan were each equivalent to just about 10,000 kilotons of TNT. "Those were the little guys," Morse said. "Those were small bombs, and they were bad enough." Hydrogen bombs, he said, would result in a yield of about 100,000 kilotons of TNT, up to several million kilotons of TNT, which would mean more deaths.

Hydrogen bombs are also harder to produce but lighter in weight, meaning they could travel farther on top of a missile, according to experts.

What are the similarities between hydrogen bombs and atomic bombs?

Both bombs are extremely lethal and have the power to kill people within seconds, as well as hours later due to radiation. Blasts from both bombs would also instantly burn wood structures to the ground, topple big buildings and render roads unusable.

[LIFE magazine](#) described such devastation in an article published on March 11, 1946, on the aftermath of the atomic bombs dropped on Japan. The piece read: "In the following waves [after the initial blast] people's bodies were terribly squeezed, then their internal organs ruptured. Then the blast blew the broken bodies at 500 to 1,000 miles per hour through the flaming, rubble-filled air. Practically everybody within a radius of 6,500 feet was killed or seriously injured and all buildings crushed or disemboweled."

Trump Questions Nuclear Deal After Iran Tests New Ballistic Missile

Source: <https://www.globalsecurity.org/wmd/library/news/iran/2017/iran-170924-rferl01.htm>

Sept 24 – U.S. President Donald Trump says Iran's test-launch of a new ballistic missile shows a landmark nuclear deal over the issue is questionable and that the Middle Eastern country is colluding with North Korea.

"Iran just test-fired a Ballistic Missile capable of reaching Israel. They are also working with North Korea. Not much of an agreement we have!" Trump said in a tweet posted late on September 23.



CBRNE-TERRORISM NEWSLETTER – October 2017

Iran fired the missile, despite warnings from Washington that it was ready to ditch the agreement with the United States and other world powers.

State broadcaster IRIB carried footage of the test-firing of the Khorramshahr missile, which was first displayed at a high-profile military parade in Tehran on September 22.

"This is the third Iranian missile with a range of 2,000 kilometers," the broadcaster said as it showed footage on September 23.

State TV did not say when the test had been conducted, although Iranian officials said on September 22 that it would be tested "soon."

The unveiling of the missile came during a military parade that commemorated the 1980s Iraq-Iran War. Iranian President Hassan Rohani said during the parade that Tehran will continue its missile program and boost the country's military capacities, despite Trump's demand that Iran stop developing "dangerous missiles."

On September 19, in a speech to the United Nations General Assembly, Trump accused Iran of supporting terrorists and called Tehran's government a "corrupt dictatorship."

Trump also called for a harder line against Iran from other members of the United Nations, saying "we cannot let a murderous regime continue these destabilizing activities while building dangerous missiles." Referring to Iran's 2015 nuclear deal with six world powers, including the United States, Trump said Washington "cannot abide by an agreement if it provides cover for the eventual construction of a nuclear program."

Rohani responded to Trump remarks in his own speech to the UN General Assembly on September 20, saying Trump's speech was "ignorant, absurd, and hateful rhetoric."

Rohani said Iran will not be the first party in the nuclear accord to violate the agreement.

It wasn't immediately clear whether Trump had made a final decision to continue complying with the Iran nuclear deal, under which Tehran agreed to curb its nuclear activities in exchange for the lifting of international sanctions.

Trump's administration has twice certified that Iran is complying with its obligations under the accord.

But it also has said that Iran's missile program violates the spirit of the nuclear agreement.

Washington is due to announce on October 15 whether it considers Iran is still complying with the agreement.




Other signatories to the nuclear accord are Russia, China, Britain, France, and Germany.

Washington has imposed unilateral sanctions against Iran, saying Tehran's ballistic-missile tests violated a UN resolution that endorsed the nuclear deal and called on Tehran not to undertake activities related to ballistic missiles capable of delivering nuclear weapons.

Tehran insists its missile program doesn't violate the resolution, saying the missiles are not designed to carry nuclear weapons.

Radiation Emergencies website

Source: <https://emergency.cdc.gov/radiation/>

Protect Yourself and Your Family	Radiation and Health Effects	Information for Professionals
 <ul style="list-style-type: none"> • In a Radiation Emergency: <ul style="list-style-type: none"> ◦ Get Inside ◦ Stay Inside ◦ Stay Tuned • Decontamination • Types of Radiation Emergencies • Preparing for Emergencies 	 <ul style="list-style-type: none"> • It's All About the Dose • Effects of Radiation Exposure and Contamination • Treatments and Countermeasures • Health Information for Pregnant and Nursing Women 	 <ul style="list-style-type: none"> • Information for: <ul style="list-style-type: none"> ◦ Clinicians ◦ Public Health Professionals ◦ Medical Examiners & Coroners ◦ Communication & Media Professionals • Guidance, Training, and Tools • Radiation Emergency Tool Kits • Radiation Emergency Resource Library



CBRNE-TERRORISM NEWSLETTER – October 2017

The Madman Theory of North Korea

By Steven Coll

Source: <http://www.homelandsecuritynewswire.com/dr20170925-the-madman-theory-of-north-korea>

Sept 26 – By the fall of 1969, President Richard Nixon had become increasingly frustrated with the refusal of North Vietnam to engage in meaningful negotiations with the United States. He believed that the Soviet Union was the only country able to persuade the North Vietnamese leadership to be forthcoming – but



how do you get the Kremlin to apply pressure on North Vietnam? Nixon's idea: To convince Leonid Brezhnev that Nixon was a madman, capable of irrational action.

Steve Coll [writes](#) in the *New Yorker* that in late October, Nixon ordered an operation code-named Giant Lance. B-52 bombers loaded with atomic weapons took off from bases in California and Washington State and headed toward the Soviet Union, then flew in loops above the polar ice cap. Nixon hoped that Soviet intelligence would interpret the action as an immediate, and completely insane, threat of nuclear attack.

Nixon confided in his chief of staff, H. R. Haldeman: "I call it the Madman Theory.... 'We'll just slip the word to them that 'for God's sake, you know Nixon is obsessed about Communism. We can't restrain him when he is angry—and he has his hand on the nuclear button.'"

President Donald Trump may be reviving Nixon's Madman Theory vis-à-vis North Korea. Coll writes:

Never before have two leaders in command of nuclear arsenals more closely evoked a professional wrestling match. It is unsettling that with both men it is hard to know where performance ends and personality begins. Trump rages publicly at Kim, but, then, he rages at everyone, from his staff to Meryl Streep. Kim may not be suicidal, but he has executed his uncle and is reported to have ordered the murder of his half brother.

In the history of nuclear diplomacy, no nation-state has ever given up atomic weapons in response to shrill threats. In a number of instances, however, countries have been coaxed to mothball their nuclear programs in exchange for political and economic returns. After the fall of the Berlin Wall, South Africa, Brazil, Argentina, Ukraine, Kazakhstan, and Belarus voluntarily gave up their nuclear weapons or abandoned advanced programs. In 2003, Muammar Qaddafi, the Libyan dictator, agreed, in exchange for economic opportunities, to surrender his uranium-enrichment equipment. Nearly twelve years later came the landmark accord in which Iran agreed to freeze its nuclear-weapons program and dismantle parts of it, in exchange for relief from sanctions.

It is not Trump's fault that North Korea has crossed ominous nuclear thresholds this year... [But] to apply some version of the Madman Theory to the North Korean problem, however, as Trump seems inclined to do, is foolish.... If Kim Jong Un believes that Trump is rash enough to initiate a first strike, he may accelerate his missile and nuclear-bomb tests and deployments. North Korea's missile-testing binge this year has increased the odds of an accident. One of Kim's rockets could veer off course and kill civilians in Japan or elsewhere. The result of such a calamity could conceivably be a war.

....

"To overcome the perils of the present," the President said at the U.N. last week, "we must begin with the wisdom of the past." If only there were some evidence that Trump knew what that was, or how to use the power of his office to forge a less dangerous world.

►► Read the full article at [New Yorker](#) (2 October 2017)

Steve Coll, a staff writer, is the dean of the Graduate School of Journalism at Columbia University, and reports on issues of intelligence and national security in the United States and abroad. For the magazine, he has written about the education of Osama bin Laden, secret negotiations between India and Pakistan over Kashmir,



and the hunt for the fugitive Taliban leader Mullah Mohammad Omar. He was the managing editor of the Washington Post from 1998 to 2005, having earlier been a feature writer, a foreign correspondent, and an editor there; in 1990, he shared a Pulitzer Prize with David Vise for a series of articles about the Securities and Exchange Commission. His book *"The Bin Ladens: An Arabian Family in the American Century"* won the PEN/John Kenneth Galbraith Award for Nonfiction; his other books include *"Ghost Wars: The Secret History of the CIA, Afghanistan, and Bin Laden, from the Soviet Invasion to September 10, 2001,"* for which he received an Overseas Press Club Award and a Pulitzer Prize; *"Private Empire: ExxonMobil and American Power"*; *"On the Grand Trunk Road: A Journey Into South Asia"*; *"Eagle on the Street,"* which was based on his reporting on the S.E.C.; *"The Taking of Getty Oil"*; and *"The Deal of the Century: The Breakup of AT&T."* From 2007 to 2013, he was the president of the New America Foundation.

Nazi Nukes: Man Finds Radioactive Evidence of Possible Nazi Atom Bomb

Source: <https://sputniknews.com/europe/201709241057644120-nazi-nuke-found-oranienburg/>

Sept 24 – **A German treasure hunter accidentally found what could be evidence that the Third Reich was closer to developing an atomic bomb than originally thought.**

A 64-year-old treasure hunter from Brandenburg, Germany, named Bernd Thälmann, stumbled upon an uncommon find while scouring ground around the town of Oranienburg.

A shiny piece of metal triggered his metal detector and, upon closer inspection, the nondescript piece of metal turned out to be non-magnetic. The find was different from what Thälmann, who has been scouring the region for some time, expected to find.

The treasure hunter brought the piece home and went to the internet for more information. What he found made him call the authorities as, upon deeper study, the metal was revealed to be highly radioactive.

According to media reports, authorities came with hazmat suits and a fire brigade, cordoned off Thälmann's house, and those of 15 neighbors, and took Thälmann into custody. Despite that he sounded the alarm, he was detained for the alleged illegal possession of radioactive materials.

According to a report by the Sunday Express, the find originated from a secret Nazi plant

located some 40 miles from Oranienburg. This plant was used by the Nazi-era Degussa company for the development of industrial-scale, high-purity uranium oxides. Degussa was, notoriously, the company that produced Zyklon B gas used to poison people in Nazi death camps.

Despite being top secret, Hitler's nuclear program was known to the Allies, who sought to sabotage or destroy it at all costs. The original facility near Oranienburg was obliterated by airstrikes estimated to have dropped some 10,000-16,000 bombs on it. Reportedly scoured by the Soviet forces after their 1945 victory, the facility was believed to have been completely destroyed.

Thälmann refused to tell police the exact location of his find, according to media reports, intending to return and continue his searches. Judges have yet to determine whether they will set charges against the treasure hunter.





Getty Images

The question of whether the Third Reich successfully developed and tested an atomic bomb before the end of the World War II is a matter of some debate. There are rumors of at least one successful test, while other sources claim that the Nazis tested as many as three bombs.

According to papers released by the US National Archives earlier this year, a German test pilot named Hans Zinsser testified that he saw a 'mushroom cloud' near a nuclear research facility at Ludwigslust in 1944.

"A cloud shaped like a mushroom with turbulent, billowing sections (at about 7000 meters) stood, without any seeming connections over the spot where the explosion took place. Strong electrical disturbances and the impossibility to continue radio communication as by lightning turned up," according to his logbook.



Will North Korea sell its nuclear technology?

By Daniel Salisbury

Source: <http://www.homelandsecuritynewswire.com/dr20170926-will-north-korea-sell-its-nuclear-technology>

Sept 26 – Earlier this month CIA Director [Mike Pompeo suggested](#) "the North Koreans have a long history of being proliferators and sharing their knowledge, their technology, their capacities around the world."

[My research has shown](#) that North Korea is more than willing to breach sanctions to earn cash.



A checkered history

Over the years North Korea has earned millions of dollars from the [export of arms and missiles](#), and its involvement in other [illicit activities](#) such as smuggling drugs, endangered wildlife products and counterfeit goods.

Still, there are only a handful of cases that suggest these illicit networks have been turned to export nuclear technology or materials to other states.

North Korean technicians allegedly assisted the Pakistanis in [production of Krytrons](#) [photo – left], likely sometime in the 1990s. Krytrons are devices used to trigger the detonation of a nuclear device.

Later in the 1990s, North Korea allegedly transferred cylinders of low-enriched [uranium hexafluoride \(UF6\) to Pakistan](#), where notorious proliferator [A.Q. Khan](#) shipped them onward to Libya.

UF6 is a gaseous uranium compound that's needed to create

the "highly enriched uranium" used in weapons.



CBRNE-TERRORISM NEWSLETTER – October 2017

The most significant case was revealed in 2007 when Israeli Air Force jets bombed a facility in Syria. The U.S. government [alleges](#) this was an “undeclared nuclear reactor,” capable of producing plutonium, that had been under construction with North Korean assistance since the late 1990s. [A U.S. intelligence briefing](#) shortly after the strike highlighted the close resemblance between the Syrian reactor and the North Korean [Yongbyon reactor](#). It also noted evidence of unspecified “cargo” being transported from North Korea to the site in 2006.

More recently, [a 2017 U.N. report](#) alleged that North Korea had been seeking to sell Lithium-6 (Li-6), an isotope used in the production of thermonuclear weapons. The online ad that caught the attention of researchers [suggested](#) North Korea could supply 22 pounds of the substance each month from Dandong, a Chinese city on the North Korean border.

There are striking similarities between this latest case and other recent efforts by North Korea to market arms using companies [“hidden in plain sight.”](#)

The Li-6 advertisement was allegedly linked to an alias of a North Korean state arms exporter known as [“Green Pine Associated Corporation.”](#) Green Pine and associated individuals [were hit](#) with a U.N. asset freeze and travel ban in 2012. The individual named on the ad was a North Korean based in Beijing formerly listed as having diplomatic status. As was [noted when the Li-6 story broke](#), the contact details provided with the ad were made up: The street address did not exist and the phone number didn’t work. However, prospective buyers could contact the seller through the online platform.

This case – our most recent data point – raises significant questions. Was this North Korea testing the water for future sales? Does it suggest that North Korea may be willing to sell materials and goods it can produce in surplus? Was the case an anomaly rather than representative of a trend?

A supplier in search of markets?

In the few public statements North Korea has made on the issue, it has [generally denied](#) that it will seek to export nuclear technology.

In 2006, for example, a Foreign Ministry official [suggested that](#) the country would “strictly prohibit any threat of ... nuclear transfer.” The U.N. sanctions regime would also [prohibit the export](#) of nuclear technologies – although North Korea has been happy to defy the U.N. regime since its inception that same year.

Additionally, there have been significant developments in states which were customers, or have been rumored to have an interest, in North Korean nuclear technology in the past.

- Syria has spent the past six years in a chaotic civil war. Since the 2007 bombing of the reactor, the country has shown no public signs of interest in nuclear weapons.
- After giving up its nuclear ambitions [in a 2003 deal](#) Libya has seen significant political changes and unrest following the collapse of the Qaddafi regime in 2011.
- The [2015 nuclear deal](#) with Iran saw the country agree to limit its nuclear program in exchange for sanctions relief, and procure nuclear technology through a [dedicated channel](#). If it continues to adhere to the deal, it has no need for illicit nuclear purchases. While some analysts [have speculated](#) about nuclear transfers from North Korea to Iran, no public evidence supports this. It’s unclear to what extent the Iran deal will survive the whims of the Trump administration, and what the longer-term implications are for Iran’s program and other states who may seek to acquire nuclear technology as a [“hedge”](#) against Iran in the region.
- Myanmar, another country with unfounded allegations of past [North Korean nuclear collaboration](#), has undergone significant political change and has made efforts to wean itself off imports of North Korean arms.

In other words, it’s unclear who – if anyone – would buy North Korean nuclear technology. However, the nightmare scenario of North Korea selling it to the highest bidder merits consideration.

It would not be the first time that an illicit procurement network turned to sales. Pakistani nuclear scientist A.Q. Khan [shifted his attention from](#) procurement for Pakistan’s program in the 1970s and 1980s to sales to Iran, Libya and North Korea in the 1980s, 1990s and 2000s. The efforts of his network saw centrifuge enrichment technology, and even a weapons design, transferred in some of the most damaging transactions ever for the nonproliferation regime.

Following the discovery of the Khan network, the U.N. and others developed better export controls, and capabilities to detect, inspect and interdict shipments. The international



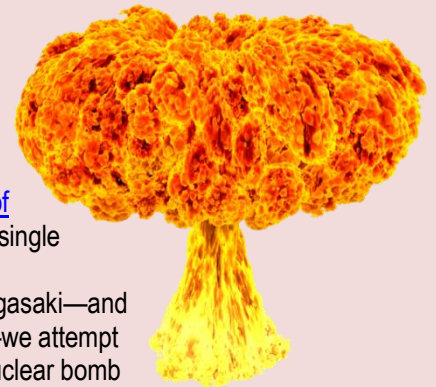
community is better prepared; however, many challenges remain in preventing illicit nuclear-related trade.

Daniel Salisbury is Stanton Nuclear Security Fellow at the Belfer Center, Harvard University.

The effects of a single terrorist nuclear bomb

By Matthew Bunn and Nickolas Roth

Source: <http://thebulletin.org/effects-single-terrorist-nuclear-bomb11150>



Sept 28 – The escalating threats between North Korea and the United States make it easy to forget the “nuclear nightmare,” as former [US Secretary of Defense William J. Perry](#) put it, that could result even from the use of just a single terrorist nuclear bomb in the heart of a major city.

At the risk of repeating the vast literature on the tragedies of Hiroshima and Nagasaki—and the substantial literature surrounding nuclear tests and simulations since then—we attempt to spell out here the likely consequences of the explosion of a single terrorist nuclear bomb on a major city, and its subsequent ripple effects on the rest of the planet. Depending on where and when it was detonated, the blast, fire, initial radiation, and long-term radioactive fallout from such a bomb could leave the heart of a major city a smoldering radioactive ruin, killing tens or hundreds of thousands of people and wounding hundreds of thousands more. Vast areas would have to be evacuated and might be uninhabitable for years. Economic, political, and social aftershocks would ripple throughout the world. A single terrorist nuclear bomb would change history. The country attacked—and the world—would never be the same.

The idea of terrorists accomplishing such a thing is, unfortunately, not out of the question; it is far easier to make a crude, unsafe, unreliable nuclear explosive that might fit in the back of a truck than it is to make a safe, reliable weapon of known yield that can be delivered by missile or combat aircraft. Numerous government studies have concluded that it is plausible that a sophisticated terrorist group could make a crude bomb if they got the needed nuclear material. And in the last quarter century, there have been some 20 seizures of stolen, weapons-usable nuclear material, and at least two terrorist groups have made significant efforts to acquire nuclear bombs.

Terrorist use of an actual nuclear bomb is a low-probability event—but the immensity of the consequences means that even a small chance is enough to justify an intensive effort to reduce the risk. Fortunately, since the early 1990s, countries around the world have significantly reduced the danger—but it remains very real, and there is more to do to ensure this nightmare never becomes reality.

Brighter than a thousand suns

Imagine a crude terrorist nuclear bomb—containing a chunk of highly enriched uranium just under the size of a regulation bowling ball, or a much smaller chunk of plutonium—suddenly detonating inside a delivery van parked in the heart of a major city. Such a terrorist bomb would release as much as 10 kilotons of explosive energy, or the equivalent of 10,000 tons of conventional explosives, a volume of explosives large enough to fill all the cars of a mile-long train. In a millionth of a second, all of that energy would be released inside that small ball of nuclear material, creating temperatures and pressures as high as those at the center of the sun. That furious energy would explode outward, releasing its energy in three main ways: a powerful blast wave; intense heat; and deadly radiation.

The ball would expand almost instantly into a fireball the width of four football fields, incinerating essentially everything and everyone within. The heated fireball would rise, sucking in air from below and expanding above, creating the mushroom cloud that has become the symbol of the terror of the nuclear age. The ionized plasma in the fireball would create a localized electromagnetic pulse more powerful than lightning, shorting out communications and electronics nearby—though most would be destroyed by the bomb’s other effects in any case. (Estimates of heat, blast, and radiation effects in this article are drawn primarily from Alex Wellerstein’s “[Nukemap](#),” which itself comes from declassified US government data, such as the government textbook [The Effects of Nuclear Weapons](#).)

At the instant of its detonation, the bomb would also release an intense burst of gamma and neutron radiation which would be lethal for nearly everyone directly exposed within about two-thirds of a mile from the center of the blast. (Those who happened to be shielded by



CBRNE-TERRORISM NEWSLETTER – October 2017

being inside, or having buildings between them and the bomb, would be partly protected—in some cases, reducing their doses by ten times or more.)

The nuclear flash from the heat of the fireball would radiate in both visible light and the infrared; it would be “brighter than a thousand suns,” in the words of the title of a book describing the development of nuclear weapons—[adapting a phrase from the Hindu epic the Bhagavad-Gita](#). Anyone who looked directly at the blast would be blinded. The heat from the fireball would ignite fires and horribly burn everyone exposed outside at distances of nearly a mile away. (In the Nagasaki Atomic Bomb Museum, visitors gaze in horror at the bones of a human hand embedded in glass melted by the bomb.)

No one has burned a city on that scale in the decades since World War II, so it is difficult to predict the full extent of the fire damage that would occur from the explosion of a nuclear bomb in one of today's cities. Modern glass, steel, and concrete buildings would presumably be less flammable than the wood-and-rice-paper housing of Hiroshima or Nagasaki in the 1940s—but many questions remain, including exactly how thousands of broken gas lines might contribute to fire damage (as they did in Dresden during World War II). On 9/11, the buildings of the World Trade Center proved to be much more vulnerable to fire damage than had been expected. Ultimately, even a crude terrorist nuclear bomb would carry the possibility that the countless fires touched off by the explosion would coalesce into a devastating firestorm, as occurred at Hiroshima. In a firestorm, the rising column of hot air from the massive fire sucks in the air from all around, creating hurricane-force winds; everything flammable and everything alive within the firestorm would be consumed. The fires and the dust from the blast would make it extremely difficult for either rescuers or survivors to see.

The explosion would create a powerful blast wave rushing out in every direction. For more than a quarter-mile all around the blast, the pulse of pressure would be over 20 pounds per square inch above atmospheric pressure (known as “overpressure”), destroying or severely damaging even sturdy buildings. The combination of blast, heat, and radiation would kill virtually everyone in this zone. The blast would be accompanied by winds of many hundreds of miles per hour.

The damage from the explosion would extend far beyond this inner zone of almost total death. Out to more than half a mile, the blast would be strong enough to collapse most residential buildings and create a serious danger that office buildings would topple over, killing those inside and those in the path of the rubble. (On the other hand, the office towers of a modern city would tend to block the blast wave in some areas, providing [partial protection](#) from the blast, as well as from the heat and radiation.) In that zone, almost anything made of wood would be destroyed: Roofs would cave in, windows would shatter, gas lines would rupture. Telephone poles, street lamps, and utility lines would be severely damaged. Many roads would be blocked by mountains of wreckage. In this zone, many people would be killed or injured in building collapses, or trapped under the rubble; many more would be burned, blinded, or injured by flying debris. In many cases, their charred skin would become ragged and fall off in sheets.

The effects of the detonation would act in deadly synergy. The smashed materials of buildings broken by the blast would be far easier for the fires to ignite than intact structures. The effects of radiation would make it far more difficult for burned and injured people to recover. The combination of burns, radiation, and physical injuries would cause far more death and suffering than any one of them would alone.

The silent killer

The bomb's immediate effects would be followed by a slow, lingering killer: radioactive fallout. A bomb detonated at ground level would dig a huge crater, hurling tons of earth and debris thousands of feet into the sky. Sucked into the rising fireball, these particles would mix with the radioactive remainders of the bomb, and over the next few hours or days, the debris would rain down for miles downwind. Depending on weather and wind patterns, the fallout could actually be deadlier and make a far larger area unusable than the blast itself. Acute radiation sickness from the initial radiation pulse and the fallout would likely affect tens of thousands of people. Depending on the dose, they might suffer from vomiting, watery diarrhea, fever, sores, loss of hair, and bone marrow depletion. Some would survive; some would die within days; some would take months to die. Cancer rates among the survivors would rise. Women would be more vulnerable than men—children and infants especially so.

Much of the radiation from a nuclear blast is short-lived; radiation levels even a few days after the blast would be far below those in the first hours. For those not killed or terribly wounded by the initial explosion, the best advice would be to take shelter in a basement for at least several days. But many would be too terrified to stay. Thousands of panic-stricken



CBRNE-TERRORISM NEWSLETTER – October 2017

people might receive deadly doses of radiation as they fled from their homes. Some of the radiation will be longer-lived; areas most severely affected would have to be abandoned for many years after the attack. The combination of radioactive fallout and the devastation of nearly all life-sustaining infrastructure over a vast area would mean that hundreds of thousands of people would have to evacuate.

Ambulances to nowhere

The explosion would also destroy much of the city's ability to respond. Hospitals would be leveled, doctors and nurses killed and wounded, ambulances destroyed. **(In Hiroshima, 42 of 45 hospitals were destroyed or severely damaged, and 270 of 300 doctors were killed.)** Resources that survived outside the zone of destruction would be utterly overwhelmed. Hospitals have no ability to cope with tens or hundreds of thousands of terribly burned and injured people all at once; the United States, for example, has 1,760 [burn beds](#) in hospitals nationwide, of which a third are available on any given day.

And the problem would not be limited to hospitals; firefighters, for example, would have little ability to cope with thousands of fires raging out of control at once. Fire stations and equipment would be destroyed in the affected area, and firemen killed, along with police and other emergency responders. Some of the first responders may become casualties themselves, from radioactive fallout, fire, and collapsing buildings. Over much of the affected area, communications would be destroyed, by both the physical effects and the electromagnetic pulse from the explosion.

Better preparation for such a disaster could save thousands of lives—but ultimately, [there is no way](#) any city can genuinely be prepared for a catastrophe on such a historic scale, occurring in a flash, with zero warning. **Rescue and recovery attempts would be impeded by the destruction of most of the needed personnel and equipment, and by fire, debris, radiation, fear, lack of communications, and the immense scale of the disaster.** The US military and the national guard could provide critically important capabilities—but [federal plans](#) assume that “no significant federal response” would be available for 24-to-72 hours. Many of those burned and injured would wait in vain for help, food, or water, perhaps for days.

The scale of death and suffering

How many would die in such an event, and how many would be terribly wounded, would depend on where and when the bomb was detonated, what the weather conditions were at the time, how successful the response was in helping the wounded survivors, and more. Many estimates of casualties are based on census data, which reflect where people sleep at night; if the attack occurred in the middle of a workday, the numbers of people crowded into the office towers at the heart of many modern cities would be far higher. **The daytime population of Manhattan, for example, is roughly twice its nighttime population; in Midtown on a typical workday, there are an estimated 980,000 people per square mile.** A 10-kiloton weapon detonated there might well kill half a million people—not counting those who might [die of radiation sickness from the fallout](#). (These effects were analyzed in great detail in the Rand Corporation's [Considering the Effects of a Catastrophic Terrorist Attack](#) and the *British Medical Journal*'s “[Nuclear terrorism](#).”)

On a typical day, the wind would blow the fallout north, seriously contaminating virtually all of Manhattan above Gramercy Park; people living as far away as Stamford, Connecticut would likely have to evacuate. Seriously injured survivors would greatly outnumber the dead, their suffering magnified by the complete inadequacy of available help. The psychological and social effects—overwhelming sadness, depression, post-traumatic stress disorder, myriad forms of anxiety—would be profound and long-lasting.

The scenario we have been describing is a groundburst. An airburst—such as might occur, for example, if terrorists put their bomb in a small aircraft they had purchased or rented—would extend the blast and fire effects over a wider area, killing and injuring even larger numbers of people immediately. But an airburst would not have the same lingering effects from fallout as a groundburst, because the rock and dirt would not be sucked up into the fireball and contaminated. The 10-kiloton blast we have been discussing is likely toward the high end of what terrorists could plausibly achieve with a crude, improvised bomb, but even a 1-kiloton blast would be a catastrophic event, having a deadly radius between one-third and one-half that of a 10-kiloton blast.

These hundreds of thousands of people would not be mere statistics, but countless individual stories of loss—parents, children, entire families; all religions; rich and poor alike—killed or horribly mutilated. Human suffering and tragedy on this scale does not have to be imagined;



CBRNE-TERRORISM NEWSLETTER – October 2017

it can be remembered through the stories of the survivors of the US atomic bombings of Hiroshima and Nagasaki, the only times in history when nuclear weapons have been used intentionally against human beings. The pain and suffering caused by those bombings are almost beyond human comprehension; the eloquent testimony of the [Hibakusha](#)—the survivors who passed through the atomic fire—should stand as an eternal reminder of the need to prevent nuclear weapons from ever being used in anger again.

Global economic disaster

The economic impact of such an attack [would be enormous](#). The effects would reverberate for so far and so long that they are difficult to estimate in all their complexity. Hundreds of thousands of people would be too injured or sick to work for weeks or months. Hundreds of thousands more would evacuate to locations far from their jobs. Many places of employment would have to be abandoned because of the radioactive fallout. Insurance companies would reel under the losses; but at the same time, many insurance policies exclude the effects of nuclear attacks—an item insurers considered beyond their ability to cover—so the owners of thousands of buildings would not have the insurance payments needed to cover the cost of fixing them, thousands of companies would go bankrupt, and banks would be left holding an immense number of mortgages that would never be repaid.

Consumer and investor confidence would likely be dramatically affected, as worried people slowed their spending. Enormous new homeland security and military investments would be very likely. If the bomb had come in a shipping container, the targeted country—and possibly others—might stop all containers from entering until it could devise a system for ensuring they could never again be used for such a purpose, throwing a wrench into the gears of global trade for an extended period. (And this might well occur even if a shipping container had *not* been the means of delivery.)

Even the far smaller 9/11 attacks are estimated to have caused economic aftershocks [costing almost \\$1 trillion](#) even excluding the multi-trillion-dollar costs of the wars that ensued. The cost of a terrorist nuclear attack in a major city would likely be many times higher.

The most severe effects would be local, but the effects of trade disruptions, reduced economic activity, and more would reverberate around the world. Consequently, while some countries may feel that nuclear terrorism is only a concern for the countries most likely to be targeted—such as the United States—in reality it is a threat to everyone, everywhere. In 2005, then-UN Secretary-General [Kofi Annan warned](#) that these global effects would push “tens of millions of people into dire poverty,” creating “a second death toll throughout the developing world.” One [recent estimate](#) suggested that a nuclear attack in an urban area would cause a global recession, cutting global Gross Domestic Product by some two percent, and pushing an additional 30 million people in the developing world into extreme poverty.

Desperate dilemmas

In short, an act of nuclear terrorism could rip the heart out of a major city, and cause ripple effects throughout the world. The government of the country attacked would face desperate decisions: How to help the city attacked? How to prevent further attacks? How to respond or retaliate?

Terrorists—either those who committed the attack or others—would probably claim they had more bombs already hidden in other cities (whether they did or not), and threaten to detonate them unless their demands were met. The fear that this might be true could lead people to flee major cities in a large-scale, uncontrolled evacuation. There is very little ability to support the population of major cities in the surrounding countryside. The potential for widespread havoc and economic chaos is very real.

If the detonation took place in the capital of the nation attacked, much of the government might be destroyed. A bomb in Washington, D.C., for example, might kill the President, the Vice President, and many of the members of Congress and the Supreme Court. (Having some plausible national leader survive is a key reason why one cabinet member is always elsewhere on the night of the State of the Union address.) Elaborate, classified plans for “continuity of government” have already been drawn up in a number of countries, but the potential for chaos and confusion—if almost all of a country’s top leaders were killed—would still be enormous. Who, for example, could address the public on what the government would do, and what the public should do, to respond? Could anyone honestly assure the public there would be no further attacks? If they did, who would believe them? In the United States, given the practical impossibility of passing major legislation with Congress in ruins and most of its members dead or seriously injured, [some have argued](#) for passing legislation in advance giving the government emergency powers to act—and creating procedures, for



CBRNE-TERRORISM NEWSLETTER – October 2017

example, for legitimately replacing most of the House of Representatives. But to date, no such legislative preparations have been made.

In what would inevitably be a desperate effort to prevent further attacks, traditional standards of civil liberties might be jettisoned, at least for a time—particularly when people realized that the fuel for the bomb that had done such damage would easily have fit in a suitcase. Old rules limiting search and surveillance could be among the first to go. The government might well impose martial law as it sought to control the situation, hunt for the perpetrators, and find any additional weapons or nuclear materials they might have. Even the far smaller attacks of 9/11 saw the US government authorizing torture of prisoners and mass electronic surveillance.

And what standards of international order and law would still hold sway? The country attacked might well lash out militarily at whatever countries it thought might bear a portion of responsibility. (A terrifying description of the kinds of discussions that might occur appeared in Brian Jenkins' book, [Will Terrorists Go Nuclear?](#)) With the nuclear threshold already crossed in this scenario—at least by terrorists—it is conceivable that some of the resulting conflicts might escalate to nuclear use. International politics could become more brutish and violent, with powerful states taking unilateral action, by force if necessary, in an effort to ensure their security. After 9/11, the United States led the invasions of two sovereign nations, in wars that have since cost hundreds of thousands of lives and trillions of dollars, while plunging a region into chaos. Would the reaction after a far more devastating nuclear attack be any less?

In particular, the idea that each state can decide for itself how much security to provide for nuclear weapons and their essential ingredients would likely be seen as totally unacceptable following such an attack. Powerful states would likely demand that others surrender their nuclear material or accept foreign troops (or other imposed security measures) to guard it.

That could well be the first step toward a more profound transformation of the international system. After such a catastrophe, major powers may feel compelled to more freely engage in preventive war, seizing territories they worry might otherwise be terrorist safe havens, and taking other steps they see as brutal but necessary to preserve their security. For this reason, foreign policy analyst Stephen Krasner has argued that [“conventional rules of sovereignty would be abandoned overnight.”](#) Confidence in both the national security institutions of the country attacked and international institutions such as the International Atomic Energy Agency and the United Nations, which had so manifestly failed to prevent the devastation, might erode. The effect on nuclear weapons policies is hard to predict: One can imagine new nuclear terror driving a new push for nuclear disarmament, but one could also imagine states feeling more certain than ever before that they needed nuclear weapons.

Prevention: The essential remedy

Given the horrifying consequences of such an event, while there is certainly a need to be better prepared to respond, the primary focus must be on prevention. Fortunately, there is good news on this front. To date, there is no evidence that nuclear weapons or the materials needed to make them have ever fallen into the hands of a terrorist group; even large and sophisticated terrorist groups that have tried to get nuclear weapons have failed to do so; and the international community has taken a wide range of actions over the past quarter-century (and particularly over the 2010-2016 period of the nuclear security summits) that have drastically improved the security measures for nuclear weapons and materials around the world. Nevertheless, while the chance of such a nightmare unfolding is probably small, it is certainly not small enough to justify complacency. Al Qaeda had a focused effort to acquire nuclear weapons that reported directly to Ayman al-Zawahiri, now the group's leader, and included multiple attempts to get nuclear material and recruit nuclear expertise; Al Qaeda progressed as far as carrying out crude conventional explosive tests for their bomb program in the Afghan desert. The Japanese terror cult Aum Shinrikyo—the group that launched nerve gas attacks in the Tokyo subway in 1995—also pursued nuclear weapons. To date, there are only hints of nuclear interest from the Islamic State, but if it did turn to nuclear pursuits, even with the imminent defeat of its geographic caliphate in Iraq and Syria, it still has more money, people, and ability to recruit experts globally than most past terrorist groups, raising a serious concern. With at least two terrorist groups having pursued nuclear weapons over the past quarter-century, and possibly more, it is unlikely they will be the last.

Moreover, the past seizures of stolen weapons-usable nuclear material demonstrate that nuclear security failures have occurred at some point in the past. While nuclear security has



CBRNE-TERRORISM NEWSLETTER – October 2017

improved dramatically in many countries in the past quarter-century, the possibility that terrorists could get the essential ingredients of a nuclear bomb still cannot be ruled out.

What then, must be done? First, major efforts are needed to recover some of the momentum imparted to nuclear security programs by the now-completed nuclear security summit process, revitalizing efforts to address remaining weaknesses. Second, because nuclear security is unlikely to be perfect, other layers of defense are needed to cope with nuclear material that has already been stolen, including stronger anti-nuclear smuggling efforts (especially national police and intelligence teams), better intelligence focused on nuclear smuggling, beefed-up interdiction abilities if intelligence identifies where such items are located, and improved means of detecting efforts to bring a nuclear weapon or its pieces into major cities. Third, deterrence can play a part, particularly in convincing states never to consciously provide nuclear weapons or materials to terrorists—and toward that end, continued investments in [nuclear forensics](#) capabilities are needed, to help identify where nuclear material might have come from. Fourth, more intelligence effort—and more international intelligence cooperation—is needed that is targeted on identifying and stopping terrorist plots aimed at nuclear terrorism, and dismantling groups that may harbor such ambitions.

No one knows what the real probability of nuclear terrorism is. It may well be quite low. There is no need for panic, which is exactly what terrorists have sought to achieve by repeatedly claiming to have nuclear weapons. But there is a need for prudent, focused action. Given the scale of the consequences, the countries of the world have an obligation to do everything in their power to ensure that the dark day after a terrorist nuclear blast never comes.

Matthew Bunn is a professor of practice at the Harvard Kennedy School. A former advisor in the White House Office of Science and Technology Policy, he is the author or co-author of over 20 books or major technical reports, and over 100 articles in publications ranging from Science to The Washington Post.

Nickolas Roth is a research associate at the Belfer Center's Project on Managing the Atom at Harvard University. The author or co-author of dozens of articles and reports on nuclear security, nonproliferation, and arms control, Roth is also a research fellow at the Center for International and Security Studies at the University of Maryland.

Do Flynn's nuclear dealings top Manafort's Kurdish referendum?

By Rachel Bronson

Source: <http://thebulletin.org/do-flynn%E2%80%99s-nuclear-dealings-top-manafort%E2%80%99s-kurdish-referendum11140>

Sept 25 – In what seems to be a competition among former Trump officials to see who can best undermine long-term American interests in the Middle East, the past few weeks have been a doozy to watch. The [recent revelation](#) that erstwhile Trump campaign manager Paul Manafort—already under special counsel Robert Mueller's scrutiny in regard to foreign clients—is working to promote today's Kurdish referendum on independence from Iraq should be a natural winner. The United States officially opposes this vote, and Kurdish officials that I have spoken with acknowledge that it will cause significant problems with Baghdad and provide the Kurds very few benefits. But what Kurdish leader can vote against independence? It's a no-win and all-lose situation, with lots of money attached. A perfect fit for Manafort.

But Manafort's dealings are overshadowed by [breaking news in the Wall Street Journal](#) that former National Security Adviser Michael Flynn did not disclose his involvement in a Russian-Saudi nuclear deal—worth hundreds of billions of dollars—that aims to bring civilian nuclear power to the Kingdom. The details of the deal are fuzzy, but it includes Russia building nuclear plants in Saudi Arabia, delivering reactor fuel, and removing spent fuel in an arrangement, often dubbed “buy, own, and operate,” that Moscow employs around the world. The UK's *Guardian* newspaper said the plan called for building as many as [40 nuclear reactors across the Middle East](#) through an international consortium that would include companies from the United States, Russia, and a host of other countries.

The deal has far reaching consequences; it would introduce Russian influence into Saudi Arabia's energy infrastructure, influence that has been to date negligible. It raises a series



CBRNE-TERRORISM NEWSLETTER – October 2017

of connected questions: What are the Russians up to? Why would the Saudis do this? What are US interests in this matter? And who should pursue them?

The Russian piece is fairly straightforward. The Russians are responding to requests from countries around the world for help in building nuclear power plants that could ease their energy challenges and, perhaps, offer military opportunities. As South African expert Emma Lecavalier described in [a piece for the Bulletin](#) in 2014, “Moscow quietly became the leader of the \$500 billion global nuclear energy market, building 37 percent of all new reactors in the world, eclipsing the United States’ meager 7 percent share.” Russia has recently signed deals across Europe, Latin America, South and Southeast Asia, and the Middle East.

Russian leaders clearly understand that securing a stake in a country’s energy infrastructure gives them long-term clout, and [the Middle East offers tremendous opportunity](#). In 2010, Turkey, a NATO member, signed a \$20 billion deal with Russia for four nuclear reactors. In 2015, Jordan, another traditional US ally, penned a \$10 billion agreement with Russia for two reactors. In June 2015, when Flynn first got involved, Saudi Arabia signed an agreement with Russia outlining a series of cooperative measures for building nuclear power plants.

For its part, Saudi Arabia has explored nuclear power as a way of serving the country’s growing domestic energy demand—demand now supplied via oil-fired power plants that threaten to swallow up valuable export potential. A civilian nuclear energy program could satisfy electricity demand, increase oil exports, and also serve as a quiet reminder to the Iranians that they are just one among several Gulf actors in the nuclear game, should Tehran abrogate its responsibilities under the Iran nuclear deal or reinstate its nuclear programs when the obligations outlined in the Joint Comprehensive Plan of Action sunset.

Until the Flynn revelations, the United States had been pretty quiet on the issue of Russia’s nuclear involvement in the Middle East. Washington has let the US civilian nuclear prowess wither and therefore cannot bring as much to the Middle East nuclear power bargaining table as it once did. At the same time, the United States hasn’t liked either of the fraught alternatives: helping its allies with their civilian nuclear programs or letting the Russians do it. The result has been US non-action, thereby ceding influence to Russia.

Flynn seems to have made a unilateral decision that Russia should take a leading role, and he has worked hard to facilitate it. He clearly knew that this was a controversial decision: He did not disclose his deep involvement prior to taking his top White House post, and he quietly continued his involvement once under the White House roof. Democrats like Maryland Rep. Elijah Cummings and New York Rep. Eliot Engel have [good reason](#) to want to know more.

Washington has real choices to make as it tries to figure out how to manage the future energy landscape in fragile security environments like the Middle East. But it is dangerous to let rogue actors like Mike Flynn make those decision for us. For this reason, Flynn gets my vote for this month’s most destructive actor award. An ignominious award with far too many contenders.

Rachel Bronson is the Executive Director and Publisher of the Bulletin of the Atomic Scientists where she oversees the publishing programs, the management of the Doomsday Clock, and a growing set of activities around nuclear weapons, nuclear energy, climate change and emerging technologies. Her writings have appeared in hundreds of publications including Foreign Policy, Foreign Affairs, The National Interest, The New York Times, the Washington Post, Huffington Post and The Chicago Tribune. She has appeared as a commentator on numerous radio and television outlets, including National Public Radio, CNN, al Jazeera, the Yomiuri Shimbun, PBS NewsHour, The Charlie Rose Show, and The Daily Show with Jon Stewart. Bronson has served as a consultant to NBC News and the Center for Naval Analyses. She testified before the Congressional Anti-Terrorist Finance Task Force, Congress’ Joint Economic Committee, and the 9/11 Commission. Bronson is a board director of the American University of Iraq, Sulaimani and the Truman National Security Program. She has served as cochair of Chicago Shakespeare Theater’s Producer Guild, and as a board member of the Ruth Page Center for the Arts. Bronson was named by Today’s Chicago Woman magazine as one of 100 Women to Watch (2012), 20 Women to Watch by Crain’s Chicago Business (2008), a Carnegie Corporation Scholar (2003) and a Glamour Magazine “Wow Woman” (2002). She is a member of the Council on Foreign Relations, the Economic Club of Chicago and the Pacific Council. She earned a BA in history at the University of Pennsylvania and a MA and PhD in political science from Columbia University in 1997.



How to Build Your Own Family Fallout Shelter

Source: <https://lifehacker.com/how-to-build-your-own-family-fallout-shelter-1818854562>

Climate Change Could Uncover An Abandoned Arctic Nuclear Base

Source: http://www.huffingtonpost.ca/2017/05/23/climate-change-arctic_n_16792324.html

May 25 – Climate change is causing record levels of ice to disappear from the Arctic, and the melt is unearthing something that was supposed to stay buried for centuries — an abandoned U.S. nuclear base. Camp Century was built in Greenland in 1959 during the peak of the Cold War. The subterranean base held between 85 and 200 soldiers year-round. The base was built under the pretense that it would be a centre for scientific experiments on the icecap and a space to test construction techniques in Arctic conditions.

The base was really part of "Project Iceworm," a top secret U.S. army program that intended to build a network of missile launch sites under the ice sheet.

The camp was essentially a small town under the ice. When abandoned in 1967, the trenches and buildings — including houses, a town store and even a hospital — were left behind, too.



The engineers stationed there also abandoned a nuclear generator that was "minimally" decommissioned, as they assumed it would be "preserved for eternity" by perpetual snowfall," according to a 2016 study by Geophysical Research Letters. Other than the nuclear reaction chamber, all of the infrastructure and nuclear waste at the site was left intact.

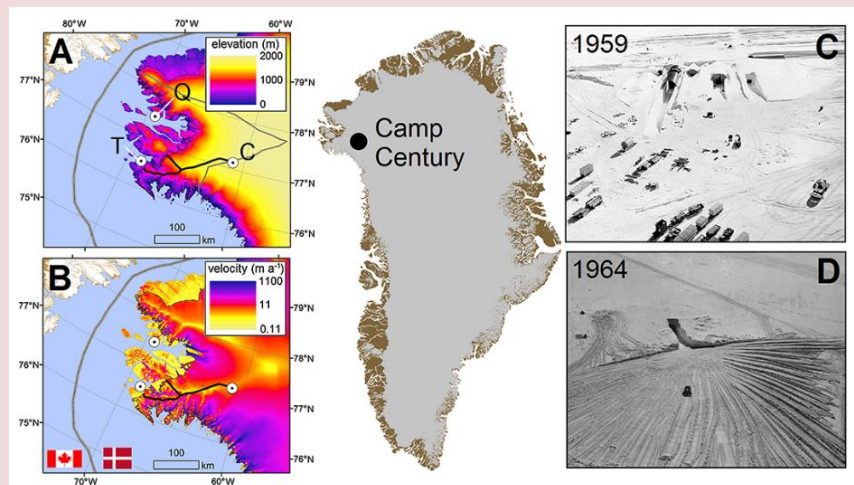
An undated photo shows the main trench to Century Camp in Greenland. (Photo: Pictorial Parade/Archive Photos/Getty Images)

The researchers weren't totally off-base with their belief that the site wouldn't melt. The camp was

established on what's known as the "dry snow zone" of the Greenland ice sheet, where almost no surface melting was known to occur at the time.

According to NASA's Earth Science Communications Team, [geoscientists in the '60s](#) believed that the climate could only change on a

large timescale, over thousands of years. It wasn't until 1979 that it was proven that increased carbon dioxide in the atmosphere would result in significant negative changes to the earth's climate.



CBRNE-TERRORISM NEWSLETTER – October 2017

Climate change is hitting the Arctic hard. Surface ice melt in Northern Canada grew by [900 per cent between 2005 and 2015](#), a recent study found, and melting glaciers have begun to release pollutants like DDT and PCBs into the environment.

If the ice melts at Camp Century, it will release an abundance of PCBs as well as other physical, chemical, biological and radiological wastes (including thousands of barrels of diesel) that could eventually be swept



to Canada through [the same Arctic currents](#) that bring spectacular icebergs to Newfoundland's coast every year.

The study from Geophysical Research Letters predicted that by 2090 ice around Camp Century will begin to melt, and it will take nearly another century before the camp is fully unearthed. But meltwater runoff could carry chemical waste into the sea as soon as the ice sheet starts melting.

Since that study was

published, scientists found that the Arctic is warming more than twice as fast as the rest of earth. The "[Snow, Water, Ice](#), and Permafrost in the Arctic" report, published in April 2017, significantly increased the projections of how fast global sea-levels will rise, meaning that ice could melt at Camp Century sooner than projected.

Cleaning up the site could also be a complicated task. The U.S. has been cleaning up [old radar sites](#) across Northern Canada, but the ownership of Camp Century is a bit less clear. According to the study, "it is unclear whether Denmark was sufficiently consulted regarding the [specific decommissioning](#) of Camp Century, and thus whether the abandoned wastes there remain U.S. property."



Measuring radiation doses in mass-casualty emergencies

By Mary Sproull, Kevin Camphausen and Gregory Koblentz

Source: <http://thebulletin.org/measuring-radiation-doses-mass-casualty-emergencies11162>

Oct 04 – For the first time since 1981, when China deployed the DF-5 intercontinental ballistic missile, a new state has gained the capability to target the United States with a nuclear weapon. On July 4 and again on July 28, North Korea launched the Hwasong-14—a two-stage, liquid-fueled ballistic missile that demonstrated the capability to reach the continental United States. The US intelligence community [assesses](#) that North Korea has nuclear warheads compact and light enough to fit on the Hwasong-14 and that North Korea will be able to deploy a nuclear-armed intercontinental ballistic missile within one or two years. North Korea demonstrated another new capability on September 3, testing what it claimed was a thermonuclear weapon. While the exact configuration of this "advanced nuclear device" remains unknown, the device's estimated yield is 140 kilotons, so the test represents a quantum leap in the destructive potential of North Korea's nuclear arsenal.

Tensions between the United States and North Korea escalated dramatically in the wake of these missile and nuclear tests. Donald Trump and Kim Jong-un engaged in a frightening war of words. The tensions prompted Hawaii, Guam, and California to increase their preparedness for a possible nuclear strike.

The medical consequences of even a single nuclear detonation would be horrific. According to [Jerome Hauer](#), former director of emergency management for New York City, no city in the United States is prepared for the casualties, chaos, and destruction that would follow a nuclear detonation. Medical management in particular would be complicated by damage to infrastructure and communication systems, lack of sufficient first responders, scarce resources, complicated triage needs, and an overwhelming number of patients.



CBRNE-TERRORISM NEWSLETTER – October 2017

But Hauer highlights another set of crucial challenges—those associated with the diagnosis and treatment of radiation-related injuries:

Beyond the difficult front lines of triage, survivors of a nuclear explosion will have a variety of injuries, some well known to modern hospitals but others more difficult to diagnose and develop a plan for. Acute radiation syndrome, in particular, results from exposure to radiation and does not have to coincide with any other injury. It may be the only effect a survivor suffers, and it may not manifest soon after exposure.

Fortunately, new types of diagnostics to address this critical need are being developed in the field of radiation biodosimetry. Radiation biodosimetry is the estimation, through observation of biological variables, of received dose from previous radiation exposure; the new diagnostics use changes in various biological markers to estimate the severity of radiation doses. Progress in radiation biodosimetry science is beginning to translate into advanced, field-deployable technologies. The United States could significantly improve its preparedness for a radiological or nuclear disaster if, while better leveraging its existing capability for biological dosimetry assessments, it also integrated emerging technologies into its radiological emergency planning and response.

Although federal guidelines for radiological emergency planning and response highlight the importance of radiation dose assessment as a core need for medical management of mass radiation exposures, the ability to rapidly and reliably measure radiation exposure in large numbers of victims is extremely limited in the United States. A 2010 [review](#) of US preparedness for a large-scale radiological event found that the United States lacked a number of key capabilities required to implement that mission, including:

- executable interagency procedures for medical triage following a radiological event
- adequate biodosimetry laboratory capacity
- a strategic plan to activate surge capacity resources for biodosimetry capability
- operational guidelines for biodosimetry sample handling and reporting
- requirements for short-term and long-term monitoring of individuals exposed to radiation
- establishment and integration of emerging high-capacity biodosimetry technologies

These capabilities would be useful for responding to the detonation of a nuclear weapon, to a “dirty bomb” attack with radioactive material, or to an accident at a nuclear power plant such as the one that occurred at Japan’s Fukushima Daichii facility in 2011. In particular, enhancing preparedness for a radiological emergency requires immediate attention in three areas: establishing a surge capacity for biodosimetry labs; developing new biodosimetry assays; and integrating biodosimetry into operational response plans.

Surge capacity

In the United States, limited laboratory and point-of-care diagnostics are available to determine if someone has been exposed to radiation and, if so, to what degree. Moreover, currently available tools are poorly suited for management of a mass-screening scenario. The only point-of-care capabilities now available for biodosimetry assessment are [lymphocyte depletion kinetics](#) (measuring the rate of depletion of white blood cells to estimate received radiation dose) and clinical evaluation. Lymphocyte depletion kinetics is not conducive to [triage biodosimetry](#) because a baseline sample is needed soon after exposure for comparison with samples collected later at predetermined points in time. Clinical evaluation for [dose assessment](#), such as time to onset of vomiting, can be useful for approximating dose—but can also be confounded by pre-existing medical conditions, psychological factors, and the effects of blast injuries. And clinical exams are of limited utility for large-scale screening due to the need for specially trained health care workers and the amount of time needed to complete exams.

The most widely used biodosimetry diagnostic is a technique not available in a point-of-care setting known as the dicentric chromosome assay. This assay, or diagnostic test, measures the number of abnormal chromosomes caused by radiation exposure to estimate received radiation dose, and is one of many types of cytogenetic assays that measure changes in chromosome structure. (Cytogenetics is “the [branch](#) of genetics that studies the structure of DNA within the cell nucleus.”) Dicentric chromosome assay is considered the “gold standard” for dose assessment, yet it is ill suited for mass screening because it requires a high level of technical skill, takes considerable time, and must be conducted in an off-site laboratory setting. The United States has only two fully operational cytogenetic biodosimetry laboratories: the Energy Department’s Radiation Emergency Assistance Center/Training Site in Oak Ridge, Tennessee and the Defense Department’s Armed Forces



CBRNE-TERRORISM NEWSLETTER – October 2017

Radiobiology Research Institute facility in Bethesda, Maryland. (Additional, auxiliary biodosimetry resources are housed at the Naval Dosimetry Center, also in Bethesda.)

To remediate the current shortage of cytogenetic laboratory capacity, the assistant secretary of preparedness and response (an official in the Health and Human Services Department) has [proposed](#) establishing a national cytogenetic biodosimetry network. This network would encompass approximately 150 existing clinical cytogenetics laboratories that routinely perform cytogenetic assays to check for birth defects and to detect and diagnose cancer. Ideally, this proposed Integrated Clinical Diagnostics System would increase the nation's biological dose assessment capability and would, to support triage during a radiological event, include the use of dicentric chromosome assay and lymphocyte depletion kinetics.

Automated platforms for cytogenetic biodosimetry are also under development. These platforms, such as the [Rapid Automated Biodosimetry Tool](#), will adapt dicentric chromosome assay and other cytogenetic assays for mass-casualty screening. Increasing the number and capacity of laboratories capable of conducting this type of biodosimetry on a large scale is urgently needed. The Laboratory Response Network under the Centers for Disease Control and Prevention has substantial laboratory resources available for chemical and biological events, but not for radiological events.

New assays

Due to the recognized limitations of current biodosimetry assessment capabilities in the United States, government entities such as the Biomedical Advanced Research and Development Authority and the Radiation and Nuclear Countermeasures Program at the National Institutes of Health have funded research designed to identify novel biomarkers of radiation exposure. This research also facilitates late-stage development of biodosimetry devices that have the potential to quantify received radiation dose in a mass-screening setting. As a result of these funding initiatives, biodosimetry research has evolved from a relatively limited field of cytogenetic assessment (primarily depending on dicentric chromosome assay and evaluation of clinical symptoms) into a robust multidisciplinary field of radiation biology research that uses a variety of methodologies.

Research models of dose assessment, using newly identified radiation biomarkers, have been developed with the goal of developing deployable point-of-care biodosimetry assays. Technologies that can provide a [point-of-care capability](#) have entered late-stage development. Novel biomarkers have even been included in human case studies of accidental radiation exposures. For example, following a 2006 [radiation accident](#) in Dakar, Senegal, 63 individuals were screened for dose assessment using a combination of classic cytogenetic biodosimetry, analysis of lymphocyte counts, and measurement of new protein and metabolite biomarkers of radiation exposure.

Integrating biodosimetry

New biodosimetry technologies are rapidly emerging, but an important question remains: how these technologies will be used in the medical response to a radiological emergency. That uncertainty can best be addressed through four concrete measures.

First, existing biodosimetry capabilities need to be better integrated into federal radiological emergency planning and response. The first step in that process should be the creation of a concept of operations (a document that describes how a system works—from the perspective of someone who will use the system) for biodosimetry diagnostics in a civilian mass-care setting. Coordinating the federal medical response to a radiological emergency will be [complex](#) under the best of circumstances. Concepts of operations for biodosimetry at the [triage level](#) have been developed on a preliminary basis, but an interagency concept of operations for deployment of biodosimetry diagnostics in a civilian mass-care setting has not been fully developed. The specialized response teams fielded by the Medical Radiobiology Advisory Team (under the Armed Forces Radiobiology Research Institute), the Energy Department's Radiation Emergency Assistance Center/Training Site, the Health and Human Services Department, and the Veterans Administration's Medical Emergency Radiological Response Team represent vital assets within any response effort for a radiological event—yet they cannot undertake the medical management of large-scale radiological exposure on their own. For a mass-casualty incident involving radiation exposures, emergency preparedness plans need to address the complexity of medical management of [radiation injury](#) and establish operational guidelines for first responders and for use of available resources and infrastructure specific to radiation injury.



CBRNE-TERRORISM NEWSLETTER – October 2017

Second, federal response teams with practical experience in medical management of radiation exposures should be equipped with a deployable point-of-care biodosimetry diagnostic capability. In a mass-casualty event, the availability of point-of-care biodosimetry diagnostics would relieve the “worried well” problem—that is, physically uninjured people who seek medical treatment due to concern that they have been exposed to radiation. Availability of point-of-care biodosimetry diagnostics would also, by differentiating those who have been exposed from those who have received no radiation exposure, reduce the strain on local medical resources. As the technology developed by the Biomedical Advanced Research and Development Authority and the Radiation and Nuclear Countermeasures Program at the National Institutes of Health matures into field-deployable systems, these new capabilities will also need to be integrated into concepts of operation for medical responses to radiological emergencies.

Third, [training](#) in medical management of radiation injuries needs to be integrated into the primary and continuing education of health care providers and first responders. This training is essential so that medical caregivers have a working knowledge of how to interpret biodosimetry diagnostics and utilize this information to guide triage and treatment. Formation of a cytogenetic radiation biodosimetry network under the proposed Integrated Clinical Diagnostics System could also provide a surge capacity for appropriately trained medical personnel in the event of a radiological emergency.

Finally, operational point-of-care response plans at the federal, state, and local levels need to be formalized for medical management of mass-casualty radiological events. These plans should better integrate biodosimetry diagnostics into the triage management work flow. Several software platforms, such as the [Biodosimetry Assessment Tool](#) produced by the Armed Forces Radiobiology Research Institute and the Radiation Emergency Medical Management [web portal](#) (managed by the Health and Human Services Department), use existing biodosimetry techniques—such as time to onset of vomiting, lymphocyte kinetics, and dicentric chromosome assay—for triage management. But these systems are not ideal for mass-casualty care. These improved plans and software platforms should be validated through tabletop and live exercises. Fully integrating biodosimetry into existing deployable medical response teams would help ensure that the complexity of the interagency response during a radiological or nuclear event does not hinder mass screening and the medical management of patients.

Duty to plan

A North Korean nuclear attack is a high-consequence event, but an event of low probability. Then again, a nuclear attack by a foreign nation is not the only radiological emergency in which advanced radiation biodosimetry capabilities would be useful. Radiological emergencies can also include nuclear power plant accidents and “dirty bomb” attacks by terrorists. As Johns Hopkins scholar Dan Hanfling and colleagues have [highlighted](#), the United States has made great strides in emergency management preparedness for nuclear events. These improvements have come through modeling of projected infrastructure impact scenarios, establishing [Protective Action Guides](#) for civilians, and developing [preliminary concepts of operations](#) for medical management of a nuclear event. Yet gaps remain in interagency planning, communicating with the public, and working toward deployable operational capabilities.

A key gap in US nuclear and radiological emergency preparedness is the lack of advanced dosimetry-based triage management. As Hanfling argues, we have a duty to plan—and “the right planning now will save countless lives after a nuclear attack.” Radiation biodosimetry is a critical element of that planning. Indeed, it is the future of radiological emergency management.

►► **Note:** An expanded version of this article will appear in the November 2017 issue (Vol. 15, No. 6) of [Health Security](#).

Kevin Camphausen is chief of the Radiation Oncology Branch at the National Cancer Institute at the National Institutes of Health. Camphausen studies the interaction of novel drugs and radiotherapy in the treatment of glioblastoma multiforme brain tumors—in the laboratory, using preclinical model systems, and in the clinic, running clinical trials. Camphausen guides the branch’s clinical/translational program, which studies the role of new agents as both radiation sensitizers and radiation protectors. Camphausen is an internationally recognized leader in his field and an expert in drug-induced tumor radiosensitization.

Gregory Koblentz is an associate professor at and director of the Biodefense Graduate Program in the Schar School of Policy and Government at George Mason University. He is also a member of the Scientists Working Group on Biological and Chemical Security at the



CBRNE-TERRORISM NEWSLETTER – October 2017

Center for Arms Control and Non-Proliferation. He is the author of Strategic Stability in the Second Nuclear Age and Living Weapons: Biological Warfare and International Security.

Mary Sproull is a biologist in the Radiation Oncology Branch of the National Cancer Institute at the National Institutes of Health and a doctoral candidate in the Biodefense Graduate Program at the Schar School of Policy and Government at George Mason University. Her current work at the National Institutes of Health, in the laboratory of Kevin Camphausen, is funded by the Radiation and Nuclear Countermeasures Program/National Institute of Allergy and Infectious Diseases as part of an initiative to develop new radiation biodosimetry models for dose prediction.

Nobel Peace Prize 2017

Source: <https://www.commondreams.org/newswire/2017/10/06/nobel-peace-prize-2017>

Oct 06 – It is a great honour to have been awarded the Nobel Peace Prize for 2017 in recognition of our role in achieving the Treaty on the Prohibition of Nuclear Weapons. This historic agreement, adopted on 7 July with the backing of 122 nations, offers a powerful, much-needed alternative to a world in which threats of mass destruction are allowed to prevail and, indeed, are escalating.

The **International Campaign to Abolish Nuclear Weapons (ICAN)** is a coalition of non-governmental organizations in one hundred countries. By harnessing the power of the people, we have worked to bring an end to the most destructive weapon ever created – the only weapon that poses an existential threat to all humanity.

This prize is a tribute to the tireless efforts of many millions of campaigners and concerned citizens



worldwide who, ever since the dawn of the atomic age, have loudly protested nuclear weapons, insisting that they can serve no legitimate purpose and must be forever banished from the face of our earth.

It is a tribute also to the survivors of the atomic bombings of Hiroshima and Nagasaki – the hibakusha – and victims of nuclear test explosions around the world, whose searing testimonies and unstinting advocacy were instrumental in securing this landmark agreement.

The treaty categorically outlaws the worst weapons of mass destruction and establishes a clear pathway to their total elimination. It is a response to the ever-deepening concern of the international community that any use of nuclear weapons would inflict catastrophic, widespread and long-lasting harm on people and our living planet.

We are proud to have played a major role its creation, including through advocacy and participation in diplomatic conferences, and we will work assiduously in coming years to ensure its full implementation. Any nation that seeks a more peaceful world, free from the nuclear menace, will sign and ratify this crucial accord without delay.



CBRNE-TERRORISM NEWSLETTER – October 2017

The belief of some governments that nuclear weapons are a legitimate and essential source of security is not only misguided, but also dangerous, for it incites proliferation and undermines disarmament. All nations should reject these weapons completely – before they are ever used again.

This is a time of great global tension, when fiery rhetoric could all too easily lead us, inexorably, to unspeakable horror. The spectre of nuclear conflict looms large once more. If ever there were a moment for nations to declare their unequivocal opposition to nuclear weapons, that moment is now.

We applaud those nations that have already signed and ratified the Treaty on the Prohibition of Nuclear Weapons, and we urge all others to follow their lead. It offers a pathway forward at a time of alarming crisis. Disarmament is not a pipe dream, but an urgent humanitarian necessity.

We most humbly thank the Norwegian Nobel Committee. This award shines a needed light on the path the ban treaty provides towards a world free of nuclear weapons. Before it is too late, we must take that path.

The **International Campaign to Abolish Nuclear Weapons (ICAN)** is a coalition of more than 400 non-governmental organisations in 95 countries. We are calling on governments to launch negotiations on a treaty prohibiting nuclear weapons, which would place them on the same legal footing as chemical and biological weapons and help pave the way to their complete elimination.

Airborne Radioactive Isotope Suddenly Sweeps Across Europe

Source: <https://sputniknews.com/europe/201710061058021152-radioactive-isotope-sweeps-across-europe/>

Oct 06 – An unusual amount of radioactive isotope ruthenium-106 has been detected in the airspace of Germany, Italy, Austria, Switzerland and France, according to multiple European monitors.

On October 3, the Austrian Ministry of the Environment released a statement saying small amounts of the isotope had been noticed. The amounts apparently do not pose any risk of consequence to human or environmental health.



The Swiss Federal Office of Public Health found "traces of ruthenium-106, a radioactive element with a half-life of 373.6 days, in aerosols taken from Cadenazzo, Ticino, between September 25 and October 2, 2017."



CBRNE-TERRORISM NEWSLETTER – October 2017

The levels of the isotope discovered were 17,000 times lower than "the limit of air emissions set for this radionuclide in the Radiation Protection Ordinance," France's Institute for Radiological Protection and Nuclear Security (IRSN) quoted the Swiss office as saying.

It's not presently clear from where the radioactive material originated but IRSN has initiated a review of where the material came from using retro-trajectory calculation methods.

First discovered in St. Petersburg in 1844 by Russian chemist Karl Karlovich Klaus, ruthenium's name is derived from the Medieval Latin name for Russia, Ruthenia.

Klaus started out researching residues from the platinum refinery in St. Petersburg. According to the book "The Chemistry of Ruthenium," aqua regia, a mix of hydrochloric acid and nitric acid used for refining the highest quality gold (99.999 percent) among other precious metals, left behind mysterious residues that were not soluble after the aqua regia had purified the platinum.

"From these residues, he successfully isolated a new metal, for which he retained [Gottfried Wilhelm] Osann's name of **ruthenium**, both out of respect for Osann's pioneering work, and in honor of his native Russia," authors E.A. Seddon and K.R. Seddon wrote.

According to an excerpt from an English report from an 1845 edition of "Philosophical Magazine," the scientist "states, that after an uninterrupted labour of two years' duration, he has succeeded in obtaining the above metal, which he had previously discovered, in a state of purity and by a simple process from the residues of platina."

In its solid state, ruthenium is a shiny silver metal that is used for various electronic purposes in the field of computers, as a catalyst for producing ammonia and acetic acid, for certain functions of solar panels and as part of some chemotherapy treatments for eye cancer. Ruthenium-106 is one of the most stable and least dangerous of the ruthenium isotopes.

RUTHENIUM 106

Ruthenium is part of the platinum group of metals.

It is a hard, silvery-white metal with a shiny surface.

Its melting point is about 2,300 to 2,450°C (4,200 to 4,400°F)

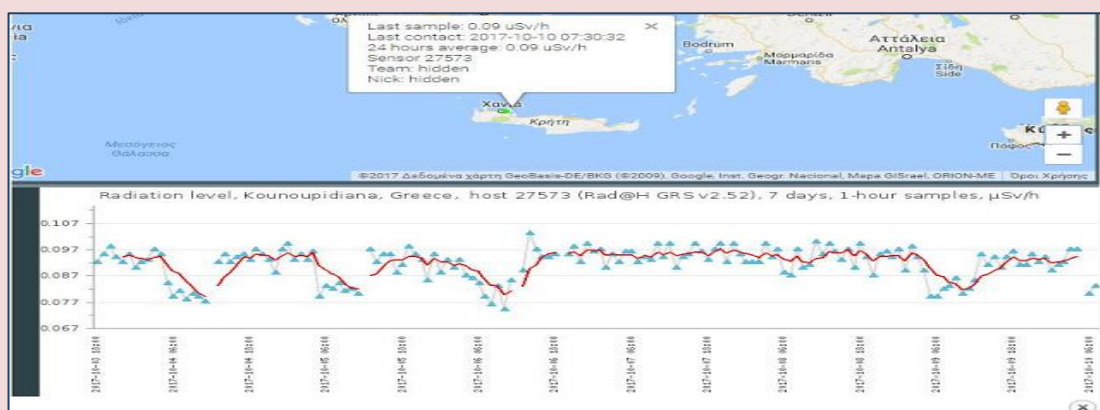
Its discovery is credited to Polish chemist Jędrzej Sniadecki, who announced the discovery of the element in 1808.

Chemists were unable to confirm Sniadecki's work and, as a result, the element was rediscovered twice more in later years.

The primary uses of ruthenium are in alloys and as catalysts for industrial processes.

Ruthenium-106 is an isotope, or variant with a different number of neutrons in its nucleus, used for radiation therapy to treat eye tumours.

It is sometimes as a source of energy, known as radioisotope thermoelectric generators, used to power satellites.



EDITOR'S COMMENT: Surveillance from Greek Atomic Energy Commission (EEAE)

revealed very low concentrations of ruthenium-106 (below 5 mBq/m³).

Consequent measurements during the 05 to 11 October period revealed concentrations lower than 0.2 mBq/m³.



Detecting nuclear materials used in dirty bombs

Source: <http://www.homelandsecuritynewswire.com/dr20171010-detecting-nuclear-materials-used-in-dirty-bombs>

Oct 10 – Imperial College London's physicists Dr. Antonin Vacheret and Dr. Sakari Ihantola have developed two devices for detecting nuclear materials.

The devices, currently being commercialized, are designed to make border security checks more effective, and also have application in environmental assessments.

Radiological material falling into the wrong hands is a constant security concern for governments around the world. Border agencies must scan incoming vehicles and freight for radioactive material, which is a challenging task, as huge volumes of both move across borders each day.

Duncan Swinscow-Hall of ICL's Institute for Security Science & Technology talked with Vacheret to find out more about the threats of radiological materials, and how his devices make detection more efficient.

Duncan Swinscow-Hall: First off, why might someone be smuggling radiological materials into a country?

Antonin Vacheret: The nightmare scenario would be terrorists deploying a dirty bomb; an explosive device that has radiological material attached to it for dispersal upon detonation.

It's important to point out that the actual number of fatalities from such an event would probably be lower than most imagine – not many more than killed by the explosion itself – the major impact would be psychological and economic.

DS-H: Have there been any incidents to date?

Vacheret: Thankfully not, although it is thought that ISIS had ideas. Back in March 2016, NPR reported that ISIS members had been following a Belgian nuclear researcher with the aim of kidnapping him to obtain the required materials.

One issue is that radiological materials are used in a variety of industrial and medical applications; the same isotopes used for life-saving medical treatments can also be used in a dirty bomb. The U.S. think tank, Nuclear Threat Initiative, reported some 514 incidents of radioactive material being lost, stolen, or is otherwise out of regulatory control from 2012-2016.

So the movement and detection of such materials is extremely important for border agencies, and is a very real challenge.

DS-H: Tell me a bit about your new devices.

Vacheret: We've developed two devices, the nFacet B and the nFacet 3D. The nFacet B model is portable, battery powered, with high neutron detection efficiency. The nFacet 3D is larger, around 15kg in weight, and provides additional 3D neutron direction measurement for source localization.

Both machines are based on new scintillator materials for neutron detection, and advanced analysis algorithms based on machine learning developed in my lab.

DS-H: What's special about these devices and why is an improvement on the current situation?

Vacheret: With incoming vehicles, the most usual situation is that they pass one by one through a gateway with neutron detectors. The first problem is that this is relatively slow, the second problem is that they tend to give false-alerts due to fluctuations in background radiation.

Our scintillator material allows incredibly sensitive detection, but our units are relatively small. The smaller of the two, the nFacet B, is designed to be portable. This allows border agents to roam among vehicles for faster detection.

The nFacet 3D is larger and not something an agent can carry, but the real benefit of this is that it gives 3D source localisation. So it can be used in an open space, help you pinpoint where the source is, and also prevent false-alarms. Examples of where this will be particularly useful would be events like the Olympic Games, or to reinforce capabilities at borders.

DS-H: You were recently awarded a NuSec grant. What was this used for?

Vacheret: We used this to further develop the software for the detectors. The software uses an algorithm to tell the user the source type and its location, which is calculated by the angle of detection. It was developed through machine learning. We basically subjected our nFacet 3D detector to reams of example radiological materials at known locations. This allowed our program to



CBRNE-TERRORISM NEWSLETTER – October 2017

learn the detection characteristics of the different events, and recognize them again with extremely high accuracy.

DS-H: What's next for nFacet?

Vacheret: We've been working with potential users to make our final product which is very close to completion. Currently we are looking for possibilities to demonstrate the capabilities of the detector in real operational environment. These demonstrations could include mounting the detector in helicopter for large-area radiation surveillance or installing the detector at a border crossing point.



ICI
International
CBRNE
INSTITUTE



EXPLOSIVE NEWS



IEDs Are More Dangerous Than Landmines

Source: <https://i-hls.com/archives/78770>

Sept 21 – Landmines have increasingly been replaced in modern warfare with improvised explosive devices, usually known as IEDs.

The mechanism of injury is the same for landmines and IEDs, while the seriousness of injuries for either device depends on how close the victim is to the center of the explosion, says a research published in BMJ Open.

Researchers suspected that pattern 1 injuries — those where the victim suffers the full effects of the explosion at close quarters — would be more serious when they involved IEDs.

They, therefore, assessed pattern 1 injuries sustained by 100 people during IED attacks in Afghanistan over 18 months in 2010-11 and compared them with pattern 1 injuries previously described for landmines. According to sciencedaily.com, IED victims were more likely than those similarly injured by landmines to have more serious injuries.

IEDs are sometimes portrayed as a primitive or crude weapon crafted from locally available resources because of a lack of access to conventional weapons, but they have evolved and are now more sophisticated, directed, and destructive, say the researchers. Just like landmines, they indiscriminately maim and kill. And that includes children, who tend to suffer the most severe injuries as a result of the powerful explosive force of an IED.

“The injury pattern suffered by the survivors of the IED is markedly worse than that of conventional [landmines],” they write. “It is a weapon, which, of its nature, causes superfluous injury and unnecessary suffering.”

The evidence gathered on the horrors inflicted by the use of landmines prompted international condemnation resulting in a ban. And the researchers conclude: “It is hoped that reports regarding the pattern of injury caused by the modern IED will result in an abhorrence of this weapon and those that use it.”

ISIS' Female Suicide Bombers Are No Myth

By Aymenn Jawad al-Tamimi

Source: <https://www.foreignaffairs.com/articles/syria/2017-09-22/isis-female-suicide-bombers-are-no-myth>

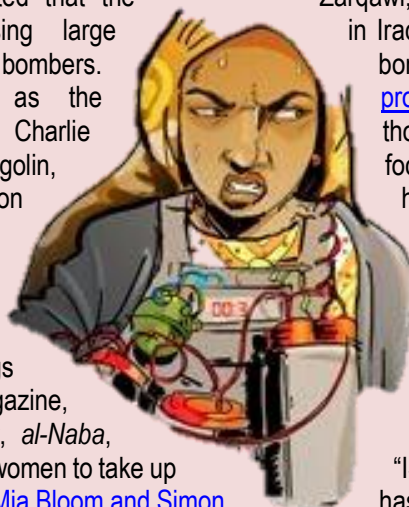
Sept 22 – In recent months, a controversy has emerged among outside analysts regarding the role of women in [the Islamic State \(or ISIS\)](#), especially after unconfirmed reports from the battle for Mosul suggested that the group had begun using large numbers of female suicide bombers.

Some analysts, such as the terrorism researchers Charlie Winter and Devorah Margolin, argue that ISIS' position on women in combat has [recently evolved](#) from prohibition to encouragement—as illustrated by some writings in the group's official magazine, *Rumiyah*, and newsletter, *al-Naba*, which in their view call on women to take up arms. On the other hand, [Mia Bloom and Simon Cottee](#) argue that this is a misreading of the relevant passages and that ISIS has

consistently prohibited women from fighting and continues to do so.

Both sides agree, however, on a supposed evolution from the time of Abu Musab al-Zarqawi, when the group (then called al Qaeda in Iraq, or AQI) openly used female suicide bombers, to the era of ISIS and its [self-proclaimed caliphate](#), when it is not thought to have engaged in the practice, focusing instead on women's role in the home and society. In other words, they draw a contrast between Zarqawi, the supposed innovator, and ISIS, which allegedly returned to more traditional gender roles. “While the precursor to ISIS, al-Qaeda in Iraq, found a more proactive role for women,” Bloom and Cottee write, “ISIS, in marked contrast, has strongly opposed any such innovation.”

Although both sides make valid points, the debate between them is



characterized by ongoing misconceptions and errors. There is no need to posit an evolution in thinking from the days of Zarqawi up to the present. Rather, the evidence suggests that ISIS and its predecessors have always considered a combat role for women to be undesirable but permissible when necessary.

What would Zarqawi do?

From the days of Zarqawi, AQI and its successors have emphasized that in most circumstances, a woman's role is to encourage her husband to wage jihad and raise her male children to be fighters, but in certain situations women may conduct operations themselves. As Winter and Margolin note, Zarqawi suggested as early as January 2004 that women could have a role in fighting—an idea he used at the time to berate men who refused to take up the cause of jihad. Later, in a speech released in July 2005, Zarqawi touched on the role of the “mujahida woman” (or woman who wages jihad), whom he described as “raising her child not to live, but to fight and be killed, then to live and be free.”

Yet Zarqawi also mentioned in the 2005 speech that “many mujahida sisters in the Land of Two Rivers [Iraq] have been sent to me, requesting to undertake martyrdom operations [suicide bombings].” Although he did not say whether he approved these requests, he once again used the example of women to shame men. “Has the disgrace in my *ummah* reached this point?,” he asked. “Have the men disappeared and thus forced us to recruit women? Is it not a disgrace on the sons of my *ummah* that our virtuous, pure sisters ask to carry out martyrdom operations while the men of my *ummah* are sleeping in their slumber and playing in their amusement?” Winter and Margolin further note that Zarqawi refers to Umm Amarah, a woman who fought for the Muslims in the Battle of Uhud in the Prophet's time, but overlook the example he cites from a battle between the Byzantines and the forces of Khalid bin al-Walid, an commander in the early Arab conquests. In the latter case, Khalid did not use the women as fighters, but rather placed them behind the army of men to supplicate to God for victory and urge on the men, while ordering these women to deny the men sexual relations should they not fight.

It is obvious from these examples that Zarqawi, like his successors, saw women first as fighters' wives and mothers, who could only undertake operations themselves in certain exceptional

circumstances. In his view, a perceived shortage of men willing to fight for the cause and the pressures brought about by the large U.S. occupation presence in Iraq justified using women as operatives and suicide bombers. By October 2005, AQI had begun claiming operations using female suicide bombers.

A change in circumstance

AQI and its earlier successors neither administered nor exercised control over contiguous territory to the extent that ISIS has since 2014. When the Islamic State of Iraq (the immediate predecessor of ISIS) announced its [appointments of cabinet ministers](#) in 2007 and 2009, the titles meant little in practice. In contrast, the various *diwans* (government departments) that ISIS set up after proclaiming its caliphate actually function on the ground, as is well attested both in the group's extensive propaganda and its internal documents. In other words, ISIS has achieved a far greater degree of *tamkin*—a concept in the jihadist context that denotes control of territory and governance—than its predecessors.

Having created its ideal state and been bolstered by an [influx of foreign fighters](#) into its ranks, ISIS has had access to an unprecedented amount of military manpower. In addition, it has not faced the vast occupying foreign armies that its predecessors dealt with in the days of the Iraq War. Thus it has generally had less need, if any, for female fighters and suicide bombers. Indeed, as Winter and Margolin suggest, the use of women in combat had already dropped off by around 2010, likely as a result the United States' gradual withdrawal of troops from Iraq. ISIS and its predecessors have always considered a combat role for women to be undesirable but permissible when necessary.

ISIS has strongly encouraged women under its control to fulfill traditional roles as wives and nurturers of children, assisting and urging on fighters for the cause both now and in the future. Yet as is evident from the 2005 speech quoted above, this line of thought is not really a divergence from Zarqawi. What is different this time is that the state project has also given women opportunities to contribute to building the Islamic State. Women in ISIS-controlled territory have been allowed to work in *hisba* (Islamic morality enforcement) teams; as teachers, doctors, and nurses; and



CBRNE-TERRORISM NEWSLETTER – October 2017

even in Islamic theological investigation and research, as in the case of [Dr. Imaan Mustafa al-Bagha](#), a Syrian woman who studied Islamic jurisprudence in Saudi Arabia before migrating back to Syria to join the Islamic State. She is said to have participated in studies by the Fatwa Issuing and Research department in Raqqa, and to have helped organize women's *hisba* teams in the provinces.

This change in circumstances, however, never meant that ISIS had outright prohibited female combatants and suicide bombers. Bloom and Cottee assert that there has been no mention of female suicide bombers in the group's discourse. This claim is incorrect. It is true, as

eastern Syria. And it has not formally acknowledged that Amaq News Agency is affiliated with ISIS, despite it being clear to almost all outside observers that the agency is part of the group's media apparatus.

In any case, ISIS' discourse has in fact mentioned female suicide bombers and military operatives in a series of internal propaganda publications distributed under the title [Stories of the Mujahideen](#). Principally designed to raise the morale of ISIS fighters, the series features stories of both men and women of the Islamic State. In keeping with the general tenor of ISIS propaganda, the female mujahideen are primarily wives and sometimes *hisba* members,



they say, that ISIS' external propaganda has never included "images of burqa-clad warriors" in its reports on martyrdom operations and other attacks, preferring instead to feature photographs and descriptions of male operatives. But the whole point of these images is to illustrate the diversity of ages and origins among ISIS fighters. This would be impossible to do with female operatives, given the group's prohibition on showing their faces. Besides, ISIS, for a variety of reasons, does not report on or declare everything to the outside world relating to its operations and functioning. For instance, the organization has said little about its presence in, and recent eviction from, the western Qalamoun border areas between Syria and Lebanon, or the deal it struck with Hezbollah and the Syrian government to send its remaining fighters and their families by bus to

caring for children and teaching the Islamic religion. But there is also a passing reference to a female suicide bomber who supposedly targeted a Kurdish YPG base in Kobani. One story focuses on Umm Fatima al-Rusiya, who supposedly had three sons who died fighting in Afghanistan and Chechnya. According to the story, she eventually took part in an assault on Grozny in December 2014 after giving allegiance to ISIS.

One should treat these stories with caution when it comes to assessing their factual content, considering their propagandistic purpose. But the fact that they mention women in suicide bombings and military operations at all shows that ISIS does not, contra Bloom and Cottee, have a "prohibition on women's participation in combat operations"



CBRNE-TERRORISM NEWSLETTER – October 2017

that is waiting to be lifted. Rather, these references are in keeping with a consistent line that has permitted such participation under the right circumstances.

A healthy skepticism

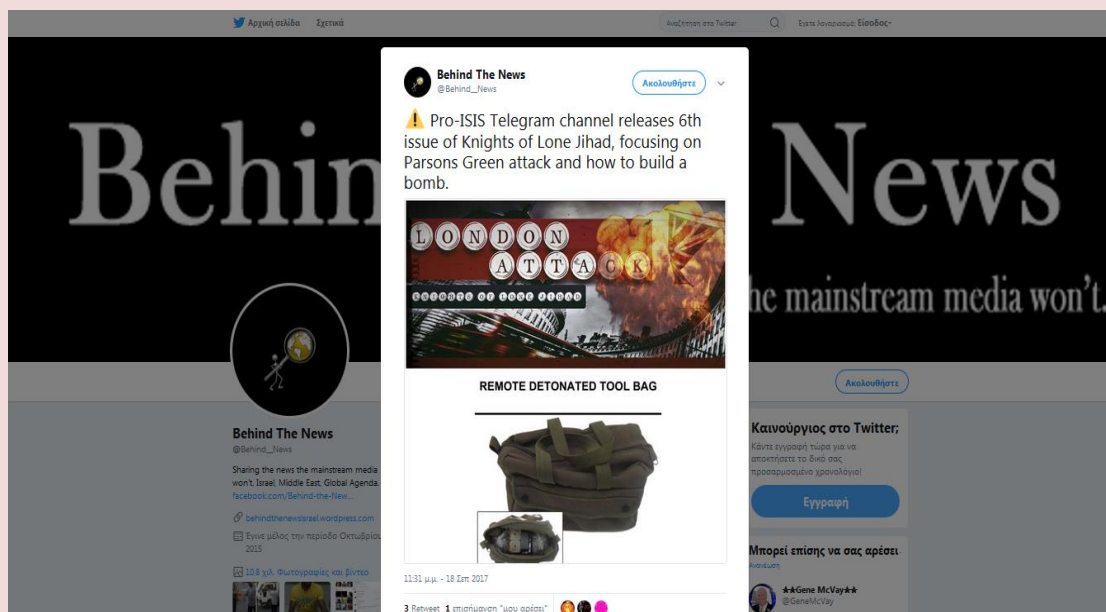
It is right to apply a healthy dose of skepticism to the reports that have come out of Mosul about ISIS' use of female suicide bombers. These could well be propaganda simply designed to blacken ISIS' image, and it is unfortunate that they were uncritically recycled in the media without proper analysis.

At the same time, in-depth analysis that purports to show a divergence between Zarqawi and ISIS on the subject of female combatants or a recent change in ISIS's own thinking on the matter is mistaken. There is no evidence of ISIS ever issuing an explicit and outright prohibition on women's participation in combat. This is evident from the various official and semi-official texts issued since ISIS' proclamation of the caliphate, which emphasize women's role in the home first

and foremost but which allow for their participation in fighting under certain conditions. In some cases—as when a woman is attacked in her own home by the enemy—fighting may in fact be an obligation.

Although here we delve into the realm of historical counterfactual, it seems likely that had Zarqawi ever realized a viable state project, he, like his successors in ISIS, would have primarily relegated women to the role of wives and nurturers of children while allowing them to contribute to similar administrative functions. Considering how ISIS reveres Zarqawi and thinks and acts in line with his ideology and methods (including his rabid anti-Shiite sectarianism and hegemonic approach to relations with other insurgent groups), there is little reason to think that it has ever disagreed with him on the issue of female suicide bombers and operatives. Continuity in outlook rather than divergence is the theme here. The only difference is the circumstance.

Aymenn Jawad al-Tamimi is a Research Fellow at the Middle East Forum, primarily focusing on Syria, Iraq and the Islamic State.



Source: https://twitter.com/Behind_News/status/910028459648409600

Cellphone bomb found hidden in passenger luggage by X-ray machine at Mangalore Airport in India

Source: <http://www.mirror.co.uk/news/cellphone-bomb-mangalore-airport-india-11202489>

Sept 21 – A cellphone 'bomb' has been discovered hidden inside a mobile phone by staff screening baggage in an X-ray machine at Mangalore Airport in India.



CBRNE-TERRORISM NEWSLETTER – October 2017

An IndiGo flight from Mangalore to Dubai was delayed this afternoon when a suspicious "clay-like" item was detected by airport scanners.

The discovery sparked a major security scare as Indian media reported a 26-year-old man travelling to Dubai had been arrested after police were called.

Early reports suggested there was confusion as to whether the device was viable or fake. Sniffer dogs reportedly gave a "mixed signal" if the item was explosive or whether it contained a chemical used to launch a possible gas attack. Indian media reported a "suspicious clay-like object" was found in the Dubai-bound passenger's mobile phone which was located in his check-in baggage.

But later it was identified as a disguise for a hand-made power pack.

Mangaluru Police Commissioner TS Suresh said: "It was a self-made power bank and after through check it was allowed to proceed," according to [Times Now News](#).

A photograph shows red and yellow electrical wires attached to a small silver object similar to a battery pack with a brown-coloured material keeping items in place.

One theory to emerge is that this was a 'dry run' by a 'terrorist sales rep' or arms dealer who was attempting to show customers how 'easy' it was to get the device onto a plane through



security - but failed.

Airline IndiGo tweeted: "IndiGo's alert security screener staff at Mangalore caught a suspect carrying alleged cellphone bomb today.

"The matter has been reported to the local police. Since it is a sensitive security matter we have nothing more to share."

India's Bureau of Civil Aviation Security (BCAS) chief Rajesh Kumar Chandra reportedly ordered the object to be investigated.

[The Times of India](#) quoted a senior aviation official who said: "The passenger, M Mohammed, was booked on IndiGo's flight 6E 877 from Mangalore to Bangalore at 10pm on Tuesday and then he was to travel from Bangalore to Dubai on IndiGo

flight 6E 95 Wednesday at 7.20am.



CBRNE-TERRORISM NEWSLETTER – October 2017

"While screening his checked in baggage at Mangalore, the screener noticed that a power bank was in his bag which looked suspicious (as it showed a green coloured thick image).

"(The screener) did a physical check and opened the power bank to check and noticed a clay like



substance in the power bank."

[Times Now News](#) reported the device was later identified as a "fake improvised explosive device".

The airline flies to 46 domestic and international destinations and its main base is at the Indira Gandhi International Airport in Delhi.

Mangalore airport operates dozens of flights to domestic and major Middle Eastern cities every day with Doha, Dubai, Kuwait and Bahrain among its most popular routes.

Mangalore Airport is one of two international hubs in the Indian state of Karnataka.

It opened on Christmas Day in 1951 and was granted international status in October 2012 - six years after the first overseas flights to Dubai.

In January last year, it was announced the Airports Authority of India had provided 17,000 sq ft of space at an old terminal building to the Indian Coast Guard as headquarters for its air operations.

The Foreign Office warns of terror plots in India especially public places "visited by foreigners".

It reads: "Terrorists are very likely to try to carry out attacks in India.

"Recent attacks have targeted public places including those visited by foreigners.

"There have been recent media reports suggesting Daesh (formerly referred to as ISIL) interest in attacking targets in India.

"There may be an increased threat to places visited by British nationals such as religious sites, markets, festival venues and beaches."

Five arrested after 'failed bomb attempt' in upmarket Paris district

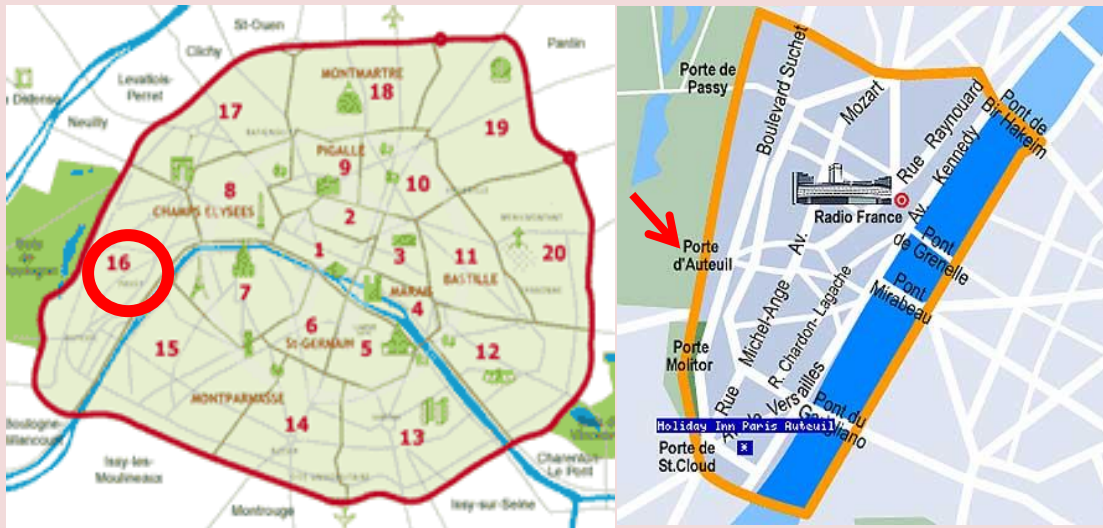
Source: <http://news.sky.com/story/five-held-after-failed-bomb-attempt-in-paris-11065308>

Oct 03 – Five people are in custody after an apparent failed bomb attempt in an upmarket district of Paris.



CBRNE-TERRORISM NEWSLETTER – October 2017

Police were alerted by a member of the public about suspicious activity in a building in the Porte d'Auteuil



neighbourhood on Saturday.

Authorities later found and deactivated an explosive device. Two gas cylinders had been discovered in the hallway of the building and two others on the pavement outside. A mobile phone attached to the cylinders was being investigated as a possible detonator, reports suggested.

An inquiry by counter-terrorism prosecutors is under way following the alert in the affluent 16th district of the French capital.

Interior minister Gerard Collomb said one of those arrested was on a police terror watchlist and had been "radicalised". Mr Collomb said the discovery of the device showed again that France was at an "extremely high" risk of terrorist attacks. French politicians are set to vote later on a new counter-terror law designed to end the country's two-year state of emergency.

Authorities would be able to place people under house arrest, order house searches and ban public gatherings without needing the prior approval of a judge.

Human rights groups and UN experts have claimed the proposed legislation gives too much power to the state.

However, Mr Collomb argued that the Paris incident and a knife attack in Marseille on Sunday that left two women dead underlined the importance of tough new security laws.

The legislation was approved by the upper house Senate in July and is set to be backed in the lower National Assembly, where the ruling centrist En Marche party has a comfortable majority.

At least 12 planned attacks in France have been foiled since the start of the year, officials claim.

The country has been under a state of emergency since the gun and bomb attacks in Paris in November 2015, which killed 130 people and left more than 400 injured.

New Police Truck is Blast and Bullet Resistant

Source: <https://i-hls.com/archives/78859>

Sept 27 – A new police truck has been one of the latest anti-terror measures in the UK Police arsenal. The armoured police vehicle is one of a state-of-the-art fleet dubbed "The Guardians", with one truck costing around £100,000, according to express.co.uk.

The police already used the bullet and blast resistant anti-terror truck to stop a "suspicious vehicle" following the recent terror attack on the Tube train. The armoured truck was first seen on the streets of London in March in the aftermath of the Westminster terror attack.

The truck is a Jankel 'Guardian', one of a fleet of Scotland Yard vans, but so far it is thought just two have been exposed. The trucks are capable of withstanding blasts from rocket-propelled grenades, hand-thrown grenades and high-calibre bullets, and can carry 10 officers.

According to mirror.co.uk, the vehicle is based on a 4x4 Ford F-450 Super Duty truck and was converted by Jankel Armouring so that it is now a seven tonne beefed-up personnel



CBRNE-TERRORISM NEWSLETTER – October 2017

carrier with wheels that are resistant to bullets and a steel floor protecting occupants from bomb explosions.



It is believed the cars contain high-tech medical equipment, weapons and sophisticated communications gear so officers can keep in touch with their operations room.

The cars have a 6.0-litre diesel engine and the windows are resistant against 7.62 calibre bullets – the ammo used by the terrorist's favourite rifle the AK47. The vehicles are equipped with super-strong smash-bars at the front so they can break their way through gates.

It seems that the UK has been taking seriously the recent terrorist attacks wave and authorities have been starting to develop various solutions suited to the type of attacks.

Petrol bomb discovered under truck in Paris in latest terror scare

Source: <http://metro.co.uk/2017/10/05/petrol-bomb-discovered-under-truck-in-paris-in-latest-terror-scare-6979414/>

Oct 05 – French media is reporting that bottles of petrol were discovered under the Franco-Swiss cement company Lafarge truck and they were connected to an ignition device. It was described as a 'crude detonator device' and was discovered in the 19th arrondissement – to the north west of the city, according to Le Figaro.



It was discovered early this morning by workers as they arrived for work.

Police and prosecutors are at the scene, according to a source close to the investigation.

Bomb disposal experts rushed to the site and police cordoned off the area, situated in a working-class district.

The incident comes as anti-terrorism police investigate

the discovery of several gas canisters and a cell phone detonator in western Paris on Saturday, but a source said there was no apparent link between the two.



CBRNE-TERRORISM NEWSLETTER – October 2017

Six people are in custody over the canisters placed in the hallway of a building in the wealthy 16th district, including two who were on watchlists for Islamic extremism.

In September last year, five full gas canisters were found in a car near the Notre Dame cathedral in central Paris.

Several women, who had received instructions from the Islamic State (IS) group to carry out an attack, were arrested.

France has suffered a series of jihadist attacks since 2015 which have left 241 people dead.

Cement giant Lafarge is under investigation over claims that it indirectly funded IS and other armed groups in Syria in order to keep a plant running in a war zone.

Earlier this year, the company admitted it had resorted to 'unacceptable practices' to continue operations at a now-closed cement factory in northern Syria in 2013-14, after most French groups had quit the war-torn country.

Inside ISIS' suicide bomb-making factories where fanatics painstakingly create deadly explosive and ball-bearing-laden vests

Source: <https://www.thesun.co.uk/news/4606391/isis-suicide-bomb-making-factory-pictures/>

Oct 03 – Wearing latex gloves, the [ISIS jihadis](#) are seen laying out plastic explosive and ball bearings as shrapnel before binding it up and stuffing it into a camouflage vest.

Another shot shows a room with several finished bombs.

A picture then shows a fighter fitted with the deadly cargo and what appears to be two triggers on the vest.

Last week it was revealed the terror group is on the run across the Middle East, according to the US led-coalition.

Col Ryan Dillon said: "ISIS is losing on all fronts, and they are losing their grip on their few remaining strongholds in both Iraq and Syria."



The coalition and its partners on the ground - the Iraqi security forces and the Syrian Democratic Forces - remain committed to defeating the enemy, he said.





"But make no mistake," Col Dillon added, "we fully expect fierce fighting in the days ahead. "And while these terrorists remain a dangerous and desperate enemy, our ISF and SDF partners have proven they are up to the task." Iraqi forces have made significant progress in the fight, Dillon said.



CBRNE-TERRORISM NEWSLETTER – October 2017

"Our Iraqi partners have fought a long, bloody war and have sacrificed a great deal to liberate their people and clear terrorists from cities and villages," he told reporters.

More than 26,000 square miles in Iraq have been cleared and more than four million people are now free from ISIS control, the colonel said.



"ISIS is on the run, and we must remain focused on delivering a decisive defeat in their few remaining holdouts in Iraq," he added.

U.S.-Born Al-Qaeda Jihadist Guilty of Plot to Use WMD to Attack U.S. Afghan Base

Source: <http://www.breitbart.com/national-security/2017/10/02/doj-al-qaeda-jihadist-guilty-conspiring-wmd-attack-american-base-afghanistan/>

Oct 02 – A U.S.-born "al-Qaeda terrorist" is facing up to life behind bars after a federal jury in New York found him guilty of conspiring to use a weapon of mass destruction (WMD) to attack an American base in Afghanistan, according to the Department of Justice (DOJ).



CBRNE-TERRORISM NEWSLETTER – October 2017

“This guy is for real, and he is a bad guy,” declared Richard Tucker, a U.S. federal prosecutor, referring to the defendant Muhanad Mahmoud al-Farekh during the closing arguments, according to the [Globe and Mail](#). “He is an honest-to-goodness al-Qaeda bad guy.”

In a [press release](#) issued after the jury convicted the defendant last Friday, DOJ identified Farekh as U.S.



citizen, noting:

A federal jury in Brooklyn, New York, returned a guilty verdict today against Muhanad Mahmoud Al-Farekh on nine counts, including conspiracy to murder U.S. nationals, conspiracy to use a weapon of mass destruction, conspiracy to bomb a government facility and conspiracy to provide material support to terrorists.

DOJ revealed that Farekh participated in several terrorist incidents overseas, including a vehicle-borne improvised explosive device (VBIED) attack back in 2009 on an American

military installation in war-devastated Afghanistan.

Farekh is a former student at the University of Manitoba located in Winnipeg, the capital of Canada's Manitoba province.

Echoing the DOJ, the *Globe and Mail* reports:

Mr. al-Farekh, an American citizen, was one of Winnipeg's “Lost Boys,” three students who mysteriously disappeared and travelled to Pakistan, sparking alarm among intelligence officials in the U.S. and Canada.

The fates of Ferid Imam and Maiwand Yar, the Canadian members of the trio, remain unknown, although Mr. Yar is believed to be dead. During the trial in New York, an RCMP [Royal Canadian Mounted Police] officer testified that neither Mr. Imam nor Mr. Yar had returned to Canada since their departure on March 6, 2007.

Farekh was reportedly born in Houston, Texas, and raised in Dubai. DOJ refers to Imam and Yar as Farekh's co-conspirators, adding that they “had become radicalized watching video recordings encouraging violent jihad, listened to jihadist lectures, including lectures by now-deceased al Qaeda in the Arabian Peninsula leader [Anwar al-Awlaki](#).”

All three former college students traveled to the **Federally Administered Tribal Areas** (FATA) of Pakistan located on the country's border with Pakistan.



FATA is “home to al Qaeda's base of operations, where they joined and received training from al Qaeda,” explains DOJ.

The United States government had considered killing him a drone strike, notes the *Globe and Mail*.

U.S. District Judge Brian M. Cogan is expected to sentence Farekh on January 11, 2018.

“Muhanad Mahmoud Al Farekh is an al Qaeda terrorist who conspired to kill Americans overseas,” proclaimed Acting U.S. Assistant Attorney General for National Security Dana Boente.

NYPD Commissioner James P. O'Neill added, “While Farekh's crimes occurred in Pakistan and Afghanistan, the defendant's co-conspirator trained Najibullah Zazi and others who also intended to attack New York City's subway system.”



CBRNE-TERRORISM NEWSLETTER – October 2017

Acting United States Attorney Bridget Rohde for the Eastern District of New York described the defendant as a "violent" member of al-Qaeda.

Fairy lights bomb plotter Zahid Hussain jailed for life

Source: <http://www.bbc.com/news/uk-england-birmingham-41556318>

Oct 09 – A man who planned to bomb a railway line with a device made from fairy lights and a pressure cooker has been jailed for life.

Zahid Hussain, 29, from Birmingham, filled the appliance with 1.6kg of shrapnel and made "improvised igniters" from the festive decorations. Hussain became radicalised reading books and websites in his bedroom.

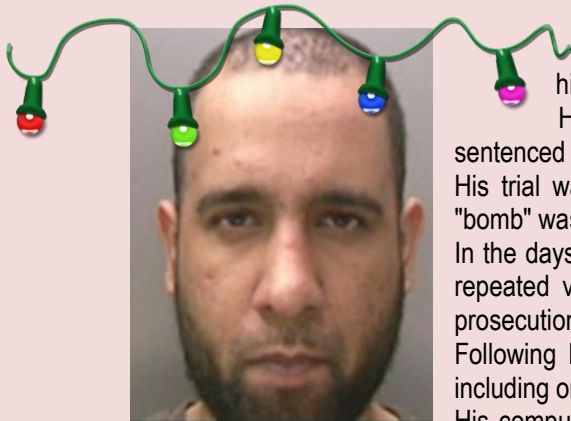
He was convicted of preparing for an act of terrorism in May and sentenced at Winchester Crown Court on Monday.

His trial was told he wrongly believed his non-viable pressure cooker "bomb" was capable of causing devastation.

In the days running up to his arrest, in August 2015, Hussain had made repeated visits to a section of the West Coast Main Line, which the prosecution said was to research a possible attack.

Following his arrest books on guerrilla warfare were also discovered, including one which talked of mounting attacks on railways.

His computer showed he had an interest in so-called Islamic State and



events in Syria.

Sentencing "dangerous" Hussain, Mr Justice Sweeney said that had his device been viable, it would have been capable of causing a "significant explosion".

The judge concluded that on the evidence and reports of several expert psychiatric reports, Hussain had - during the time of the offence - and still did, suffer with paranoid schizophrenia.

The judge said a life sentence was "appropriate" in view of "the level of the danger that you pose, and the impossibility of predicting when it will come to an end".

Hussain will serve a minimum of 15 years.



Anti-corruption blogger killed by huge bomb in Malta

Source: <https://www.reuters.com/article/us-malta-carbomb/anti-corruption-blogger-killed-by-huge-bomb-in-malta-idUSKBN1CL2A5>

Oct 16 – Daphne Caruana Galizia, Malta's best-known investigative journalist, was killed on Monday when a powerful bomb blew up her car, police said, in a case that stunned the small Mediterranean island.

Caruana Galizia, 53, ran a hugely popular blog in which she relentlessly highlighted cases of alleged high-level corruption targeting politicians from across party lines.

"There are crooks everywhere you look now. The situation is desperate," she wrote in a blog published on her site just half an hour before an explosion tore into her car.

Locals said Caruana Galizia had just left her house and was on a road near the village of Bidnija in northern Malta when the bomb detonated, sending



her car flying into an adjacent field.

Maltese Prime Minister Joseph Muscat, who faced accusations of wrong-doing by Caruana Galizia earlier this year, denounced her killing, calling it a "barbaric attack on press freedom".

He announced that the U.S. Federal Bureau of Investigation (FBI) had agreed to help local police investigate the killing and was flying experts to the island as soon as possible.

"I will not rest until I see justice done in this case," he said in a statement, calling for national unity.

Around 3,000 people held a silent, candle-lit vigil on Tuesday evening in Sliema, just outside Valletta.

The hashtag Je Suis Daphne circulated widely among social media users on the island of 400,000 people, the European Union's smallest state.

"Everyone knows Caruana Galizia was a harsh critic of mine, both politically and personally, but nobody can justify this barbaric act in any way," Muscat said. "The only remedy for anyone who felt slandered was through the courts."



CBRNE-TERRORISM NEWSLETTER – October 2017

Muscat sued Caruana Galizia after she wrote blogs earlier this year saying his wife was the beneficial owner of a company in Panama, and that large sums of money had been moved between the company and bank accounts in Azerbaijan.

Both Muscat and his wife denied the accusations.

Looking for a vote of confidence to counter the allegations, Muscat called snap elections in June which he easily won. Recently, Caruana Galizia's outspoken blog had turned its fire on opposition politicians.

Malta Television reported that Caruana Galizia had filed a complaint to the police two weeks ago to say she had received threats. It gave no further information.

Political murder

Opposition leader Adrian Delia said the blogger was the victim of a "political murder".

Slideshow (9 Images)

"Caruana Galizia revealed the Panama Papers and was the government's strongest critic," he said, calling for a independent probe of her killing.

"We will not accept an investigation by the Commissioner of Police, the Army commander or the duty magistrate, all of whom were at the heart of criticism by Caruana Galizia," he said.

WikiLeaks founder Julian Assange said he would offer a 20,000 euro (\$23,578.00) reward for information leading to the conviction of Caruana Galizia's killers, and European politicians expressed dismay at her death.

Frans Timmermans, first vice president of the European Commission, tweeted that he was "shocked and outraged", adding that "if journalists are silenced our freedom is lost".

Manfred Weber, head of the conservative bloc in the European Parliament, said the killing marked "a dark day for democracy".

Caruana Galizia took aim at politicians and senior officials from across Malta, seeing the island as a hotbed of corruption.

"Malta's public life is afflicted with dangerously unstable men with no principles or scruples," she wrote last year.

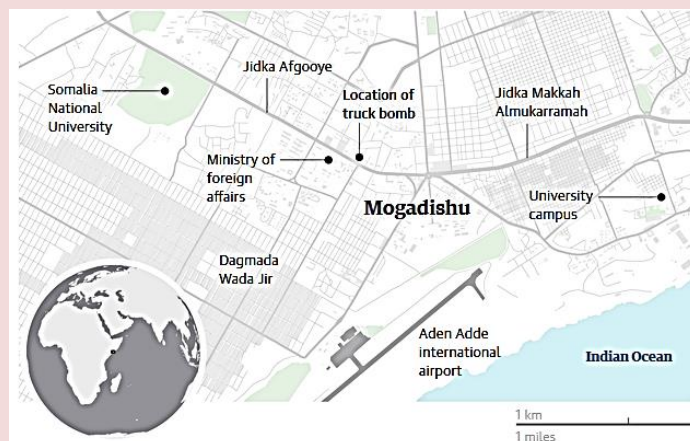
Her family asked that the magistrate assigned to investigate the case, Consuelo Scerri Herrera, be substituted because of an alleged conflict of interest, court documents showed. Herrera had sought libel damages after Caruana Galizia attacked her in her blog.

Mogadishu truck bomb: 500 casualties in Somalia's worst terrorist attack

Source: <https://www.theguardian.com/world/2017/oct/15/truck-bomb-mogadishu-kills-people-somalia>

Oct 15 – The death toll in the bombing that hit the centre of Mogadishu on Saturday continues to rise, with more than 300 people now believed to have been killed and hundreds more seriously injured.

The scale of the loss makes the attack, which involved a truck packed with several hundred kilograms of



military-grade and homemade explosives, one of the most lethal terrorist acts anywhere in the world for many years.

On Monday morning, Somalia's information minister announced that 276 people had died in the attack with at least 300 people injured. Within hours, however, Abdikadir Abdirahman, the director of Amin ambulances, said his service had confirmed that 300 people died in the blast.

"The death toll will still

be higher because some people are still missing," Abdirahman told Reuters.



CBRNE-TERRORISM NEWSLETTER – October 2017

More victims continue to be dug from the rubble spread over an area hundreds of metres wide in the centre of the city.

Rescue workers said a definitive death toll may never be established because the intense heat generated by the blast meant the remains of many people would not be found.

Others may have been buried quickly by relatives.

The devastating bombing, which provoked international condemnation, will focus attention on the decade-long battle against al-Shabaab, an Islamist group, in [Somalia](#).

Michael Keating, the UN special envoy to Somalia, called the attack “revolting”.

The US mission to Somalia said: “Such cowardly attacks reinvigorate the commitment of the United States to assist our Somali and African Union partners to combat the scourge of terrorism.”

Al-Shabab earlier this year vowed to increase its attacks after both the Trump administration and Somalia’s recently elected president announced new military efforts against the group.



Officials said more than 110 victims of the bombing had already been buried. “One hundred and sixty of the bodies could not be recognised and so they were buried by the government [on Sunday],” Aden Nur,



CBRNE-TERRORISM NEWSLETTER – October 2017

a doctor at the city's Madina hospital, said. "The others were buried by their relatives. Over a hundred injured were also brought here."

Casualties included senior civil servants, five paramedic volunteers and a journalist, but most were ordinary people on one of the busiest thoroughfares of Mogadishu, which has been hit by multiple bombings in recent years.

The bomb, which is thought to have targeted Somalia's foreign ministry, was concealed in a truck and exploded near a hotel, demolishing the building and several others.

Sources close to the Somali government said the truck had been stopped at a checkpoint and was about to be searched when the driver suddenly accelerated. It crashed through a barrier, then exploded. This ignited a fuel tanker parked nearby, creating a massive fireball.

Witnesses described bewildered families wandering among the rubble and wrecked vehicles, looking for missing relatives. Bodies were carried from the scene on makeshift stretchers made of blankets, as people tried to dig through the debris with their hands.

"There's nothing I can say. We have lost everything," said Zainab Sharif, a mother of four who lost her husband in the attack. She sat outside a hospital where he was pronounced dead after doctors tried for hours to save him from an arterial injury.

Muna Haj, 36, said: "Today, I lost my son who was dear to me. The oppressors have taken his life away from him. I hate them. May Allah give patience to all families who lost their loved ones in that tragic blast ... And I pray that one day Allah will bring his justice to the perpetrators of that evil act."

The president, Mohamed Abdullahi Mohamed, declared three days of national mourning and joined thousands of people who responded to a plea by hospitals to donate blood for the wounded. "I am appealing to all Somali people to come forward and donate," he said.

Mohamed, [who took power in February](#), had vowed to rid the country of al-Shabaab. He has faced huge challenges, with the insurgency proving resilient to the ramped-up offensive aided by the US, and a famine.



Dr Mohamed Yusuf, the director of Mogadishu's Medina hospital, said his staff had been "overwhelmed by both dead and wounded. This is really horrendous, unlike any other time in the past."

A Turkish air ambulance landed at Mogadishu airport on Monday morning to airlift 50 seriously injured people.

[Al-Shabaab](#), which has been affiliated to al-Qaida since 2011, has not yet claimed responsibility for the attack.



CBRNE-TERRORISM NEWSLETTER – October 2017

However the organisation has a history of launching bomb attacks against civilian targets in Mogadishu, and is known to avoid claiming responsibility for operations which it believes may significantly damage its public image among ordinary Somalis.

The bombing was reported on media outlets linked to al-Shabaab.

The information minister, Abdirahman Omar Osman, said: "It's a sad day. This is how merciless and brutal they are, and we have to unite against them."

One western expert working with the Somali government said the bomb was aimed at the Ministry of Foreign Affairs and it was likely al-Shabaab had not anticipated the destruction it would cause.

"That it exploded next to a fuel tanker was just very, very bad luck," the expert said.

Investigators will seek to establish the source of the military-grade explosives. One source suggested they had been stolen from Amisom, the much-criticised African Union peacekeeping mission, which has about 20,000 troops in the country.

Though largely confined to the countryside since withdrawing from Mogadishu six years ago, al-Shabaab has repeatedly taken over small towns, as well as inflicting significant losses on Amisom and Somali troops.

The US military has increased drone strikes and other efforts this year against al-Shabaab, and a US special forces operative was killed in a skirmish with the group earlier this year, the first American combat casualty in [Africa](#) since the Black Hawk episode in Mogadishu in 1993.

EDITOR'S COMMENT: 358 people dead and 400 injured BUT European mass media are SILENT the same time that they write long stories for a knife attack or a few dozens of dead/injured. But they are Africans and it does not count – isn't it? Most probably aliens from nearby planets will be puzzled and try to find logical explanations of human nature and behavior. On the other hand, in almost all sci-fi movies, our global behavior is the main reason they want to destroy us!

Dismantled Terrorist Cell: Moroccan Police Seize 'Suspicious' Chemical Substances

Source: <https://www.moroccoworldnews.com/2017/10/231078/dismantled-terrorist-cell-moroccan-police-seize-suspicious-chemical-substances/>

Oct 15 – The Moroccan Ministry of Interior revealed Saturday in a communiqué that a quantity of "suspicious" chemical substances was recovered during the operation conducted on the same day which led to the dismantling of a terrorist cell loyal to ISIS and operating in several cities.

The terrorist network operated in Fez, Casablanca, Khouribga, Zaouiat Cheikh, Sidi Bennour, Demnat, and Sidi Harazem.

[Eleven suspected terrorists](#) were arrested during police raids. The ring's leader [was arrested](#) in a "safe house" in Fez along with one of his partners. The two suspects are aged 25 and 30.

A number of weapons and explosive materials were also seized during the operation conducted by the Central Bureau of Judicial Investigations (BCIJ), the local anti-terrorism bureau.

The release stated that the chemicals substances were seized during a raid of the family house of the cell leader in Khouribga.

The confiscated material consisted of fertilizers, liquids, a thermometer, a metal tube used for making explosives and documents about how to make bombs.

The seized material will be subjected to tests by the police's forensic team, according to the Ministry.

Early investigations indicated the terrorist cell was planning to conduct attacks on key sites in the country.

The dismantled network, the Interior explained, had contacts with a field ISIS commander.

As the ministry noted, the terrorist organization has been inciting its followers to conduct attacks outside the region under its control in Syria and Iraq.

The Moroccan ring's mastermind is said to have experience in making bombs.

When BCIJ elements raided the Fez "safe house" on Saturday, three guns, two hunting rifles, live ammunition, butane gas bottles, two straps for making suicide bombs, fire extinguishers, communications equipment and large sums of cash money.

A car that belonged to one of the arrested members was reportedly seized next to the French consulate in Fez.



CBRNE-TERRORISM NEWSLETTER – October 2017

In February 2016 BCIJ [busted a terrorist cell](#) that was also suspected of planning attacks potentially involving chemical weapons.

10 suspects were arrested and the list of confiscated material included automatic machine guns, revolvers, a rifle and biological and chemical substances.

Man Tries To Board Airplane In Sweden With 'Mother Of Satan' Explosives

Source: <http://counteriedreport.com/man-tries-to-board-airplane-in-sweden-with-mother-of-satan-explosives/>

Oct 06 – A man was arrested Thursday night for allegedly attempting to bring several bags of TATP explosives onto a plane departing from **Landvetter airport in Sweden**.



TATP, also known as the “Mother of Satan,” has been used in several terror attacks across Europe in recent years. The suspect was charged with attempting public destruction.

“We have seized his belongings and we’re working on analyzing them and the suspicious items,” police spokesman Peter [Adlersson told](#) newspaper Aftonbladet.

TATP was used in deadly terror attacks in Paris in 2015 and Brussels the following year. The material caused a house to explode one day before the terror attack in Barcelona Aug. 17. Police believe the explosives were meant to be part of the attack that killed 16 people.

Swedish police did not confirm that TATP was discovered in the man’s bag.

“I have no information on what kind of material it was,” Adlersson told Aftonbladet. “Even if I did I would not say it.”

Media [reports claim](#) the suspect is a German national in his early twenties.

“We won’t reveal his nationality, but he was traveling to another country within the EU,” Adlersson said.

Explosive detection technology from a general population survey

Source: https://www.start.umd.edu/pubs/START_ExplosiveDetectionTechnologyAdoption_Infographic_October2017.pdf

A String of Bomb Blasts in Sweden Is Prompting Questions and Alt-Right Conspiracy Theories

Source: <http://time.com/4990765/sweden-bombs/>

Oct 20 – A powerful blast detonated overnight at a police station ripped off the building’s entrance. A dynamite-laced apartment doorway blew a chunk of rubble more than 250-feet away, into the living room of a neighboring building. And a provincial town was put on lockdown after a suspected car-bombing.



CBRNE-TERRORISM NEWSLETTER – October 2017

There have been at least five bomb blasts or scares in Sweden since the early hours of Friday, Oct. 13. These incidents have rocked the Scandinavian nation, and have added fuel to the alt-right's campaign to use the country as a cautionary paradigm of liberal immigration policies gone astray. Here's what you need to know.

The bombs:

No one was reportedly injured or killed in any of the incidents.

1. Overnight on [Oct. 13, a strong explosion](#) caused extensive damage to an apartment building in the Swedish city of Malmö, which has been experiencing a rise in gang violence and gun murders. In January, the area [police chief called](#) for the public's help in clamping down on mafia-like activity.
2. On Oct. 16, police, forensics experts and bomb technicians rushed to the scene after an explosion caused by a [suspected car bombing in Malmö](#).
3. An [explosion at a police station](#) in Helsingborg on Oct. 18 damaged the station entrance, and shattered windows of nearby buildings. Police have blamed the attack on criminal networks.
4. The [town of Norrköping](#) was placed on lockdown on Oct. 18 after reports of a suspected car bomb.
5. Around [9:30pm on Oct. 19](#), police received a distress call about a suspected explosive in the stairwell of an apartment building in Malmö.

Why this matters:

Crime in Sweden has become a highly politicized since U.S. President Donald Trump used the country as an example of how more open immigration policies supposedly result in upsurges of crime. In a now widely ridiculed gaffe, the president cited a non-existent incident "[last night in Sweden](#)" during a speech in February.

Alt-right talking heads have rallied around the remarks, using any episode of violence in Sweden as evidence that the president presciently exposed the nation's spiraling moral decrepitude.

**What's being said about it:**

Paul Joseph Watson, a contributor at conspiracy website [infowars.com](#) said the recent series of bombings highlight how President Trump was lambasted, "only to be proven right." He added: "Since the country accepted hundreds of thousands of Muslim migrants, low level urban terrorism has become commonplace in Sweden, which has a number of infamous Islamic ghettos."

Breitbart, which has lamented Sweden's ostensible fall from utopia to "grenade attack capital," [has speculated](#) the police station blast was an act of terrorism, even though there is no evidence that any terrorist organization was involved in any of the recent incidents.

Swedish Prime Minister Stefan Löfven called the police station blast "an attack against our democracy", and urged cops to get tougher on crime.

Malmö police chief Stefan Sinteus has suggested bolstering the local police force [with soldiers](#).

Bottomline facts:

- ◆ Incidents of reported crime [increased marginally](#) from 2015 to 2016, according to the Swedish Crime Survey, which cautions that increased claims don't necessarily mean that crime has surged.
- ◆ There is a vast gulf between [perceptions of rising crime](#), and actual crimes.



CBRNE-TERRORISM NEWSLETTER – October 2017

- ◆ Stockholm, Sweden's capital, was [just ranked](#) among the world's top ten safest cities.
- ◆ [Most offenders](#) are Swedish-born. But a government survey shows foreigners are 2.5 times more likely to be suspected of crimes.
- ◆ Sweden has accepted the [largest number](#) of asylum-seekers per capita of any European nation.
- ◆ After an [Uzbek asylum-seeker hijacked](#) a truck and plowed into Stockholm pedestrians, killing five last April, pressure has been dialed up on the government to reassess its refugee policies.





CYBER NEWS



Almost Countering misinformation and correcting “fake news”

Source: <http://www.homelandsecuritynewswire.com/dr20170925-countering-misinformation-and-correcting-fake-news>

Sept 25 – It is no use simply telling people they have their facts wrong. To be more effective at correcting misinformation in news accounts and intentionally misleading “fake news,” you need to provide a detailed counter-message with new information—and get your audience to help develop a new narrative.

Those are some takeaways from an extensive new meta-analysis of laboratory debunking studies published in the journal *Psychological Science*. The analysis, the first conducted with this collection of debunking data, finds that a detailed counter-message is better at persuading people to change their minds than merely labeling [misinformation](#) as wrong. But even after a detailed debunking, misinformation still can be hard to eliminate, the study finds.

“The effect of misinformation is very strong,” said co-author Dolores Albarracín, professor of psychology at the University of Illinois at Urbana-Champaign. “When you present it, people buy it. But we also asked whether we are able to correct for misinformation. Generally, some degree of correction is possible but it’s very difficult to completely correct.”



Countering beliefs based on misinformation

UPenn [says](#) that “Debunking: A Meta-Analysis of the Psychological Efficacy of Messages Countering Misinformation” was conducted by researchers at the Social Action Lab at the University of Illinois at Urbana-Champaign and at the Annenberg Public Policy Center of the University of Pennsylvania. The teams sought “to understand the factors underlying effective messages to counter attitudes and beliefs based on misinformation.” To do that, they examined 20 experiments in eight research reports involving 6,878 participants and 52 independent samples.

The analyzed studies, published from 1994 to 2015, focused on false social and political news accounts, including misinformation in reports of robberies; investigations of a warehouse fire and traffic accident; the supposed existence of “death panels” in the 2010 Affordable Care Act; positions of political candidates on Medicaid; and a report on whether a candidate had received donations from a convicted felon.

The researchers coded and analyzed the results of the experiments across the different studies and measured the effect of presenting misinformation, the effect of debunking, and the persistence of misinformation.

The value of extended corrections

“This analysis provides evidence of the value of the extended correction of misinformation,” said co-author Kathleen Hall Jamieson, director of the Annenberg Public Policy Center (APPC) and co-founder of its project [FactCheck.org](#), which aims to reduce the level of deception in politics and science. “Simply stating that something is false or providing a brief explanation is largely ineffective.”

The lead author, Man-pui Sally Chan, a research assistant professor in psychology at the University of Illinois at Urbana-Champaign, said the study found that “the more detailed the debunking message, the higher the debunking effect. But misinformation can’t easily be undone by debunking. The formula that undercuts the persistence of misinformation seems to be in the audience.”

A critical factor: Stimulating counterarguments among audiences

As the researchers reported: “A detailed debunking message correlated positively with the debunking effect. Surprisingly, however, a detailed debunking message also correlated positively with the misinformation-persistence effect.”

However, Albarracín said the analysis also showed that debunking is more effective - and misinformation is less persistent - when an audience develops an explanation for the



CBRNE-TERRORISM NEWSLETTER – October 2017

corrected information. “What is successful is eliciting ways for the audience to counterargue and think of reasons why the initial information was incorrect,” she said. For news outlets, involving an audience in correcting information could mean encouraging commentary, asking questions, or offering moderated reader chats - in short, mechanisms to promote thoughtful participation.

Recommendations for debunking misinformation

The researchers made three recommendations for debunking misinformation:

- Reduce arguments that support misinformation: News accounts about misinformation should not inadvertently repeat or belabor “detailed thoughts in support of the misinformation.”
- Engage audiences in scrutiny and counterarguing of information: Educational institutions should promote a state of healthy skepticism. When trying to correct misinformation, it is beneficial to have the [audience](#) involved in generating counterarguments.
- Introduce new information as part of the debunking message: People are less likely to accept debunking when the initial message is just labeled as wrong rather than countered with new evidence.

UPenn notes that the authors encouraged the continued development of “alerting systems” for debunking misinformation such as [Snopes.com](#) (fake news), [RetractionWatch.com](#) (scientific retractions), and [FactCheck.org](#) (political claims). “Such an ongoing monitoring system creates desirable conditions of scrutiny and counterarguing of misinformation,” the researchers wrote.

— Read more in Man-pui Sally Chan et al, “*Debunking: A Meta-Analysis of the Psychological Efficacy of Messages Countering Misinformation*,” [Psychological Science](#) (12 September 2017).

How does your cellphone know whether your finger is real or a fake?

Source: <http://www.homelandsecuritynewswire.com/dr20170926-how-does-your-cellphone-know-whether-your-finger-is-real-or-a-fake>



Sept 27 – **Do you know how safe it is to use your finger as a security login? And have you wondered how your cell phone knows if your finger is real or a fake?**

Michigan State University biometric expert Anil Jain and his team are working to answer these questions and solve the biggest problems facing fingerprint recognition systems today: how secure they are and how to determine whether the finger being used is actually a human finger.



CBRNE-TERRORISM NEWSLETTER – October 2017

MSU [says](#) that in an effort to test and help solve this problem, Jain, a University Distinguished Professor, and doctoral student Joshua Engelsma have for the first time designed and created a fake finger containing multiple key properties of human skin. Commonly called a spoof, this fake finger has been used to test two of the predominant types of fingerprint readers to help determine their resilience to spoof attacks. Watch the finger being made in [this video](#).

The fake fingers developed at MSU were created using a combination of carefully chosen materials, including conductive silicone, silicone thinner and pigments. In addition to determining the materials, the entire fabrication process, using a molding and casting technique, was designed and implemented by the team.

“What makes our design unique is that it mimics a real finger by incorporating basic properties of human skin,” said Jain. “This new spoof has the proper mechanical, optical and electrical properties of a human finger. Compared to current fake fingers that only contain one or two of these properties, our new version could prove much more challenging to detect. It will help motivate designers to build better fingerprint readers and develop robust spoof-detection algorithms.”

Developing more resilient fingerprint readers is important because they are now abundantly used for authentication in cell phones, computers, amusement parks, banks, airports, law enforcement, border security and more.

One specific way the synthetic fingers will be used is for testing the recognition accuracy between different types of fingerprint readers. The readers differ based on the type of sensors used to record the digital fingerprints, such as optical (using light rays to capture an image) or capacitive (using electrical current to create an image).

Currently, recognition accuracy declines when the same fingerprint taken using two different types of fingerprint readers is compared. For example, if a capacitive reader was used to capture a fingerprint, but an optical fingerprint reader was used later to authenticate that same fingerprint, it's less likely the print will be accurately identified. By using MSU's new spoof, companies could develop methods to improve the accuracy.

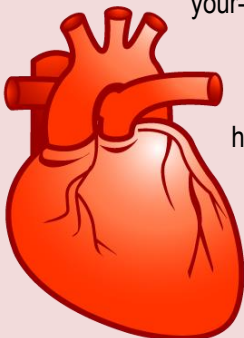
“Given their unique characteristics, we believe our fake fingers will be valuable to the fingerprint recognition community,” said Jain. “Consumers need to know their fingerprints and identity are secure, and vendors and designers need to demonstrate to the consumers the technology is not only accurate but also resilient to spoof attacks.”

Jain and his team have begun work on the next phase of this research: designing and building a fingerprint reader to test spoof-detection capabilities. Once ready, this low-cost reader could be easily built in a couple of hours by others in the fingerprint recognition community to test for real versus fake fingerprints. Jain's lab is additionally working on algorithms that will make this fingerprint reader more resilient to spoof presentation attacks.

— Read more in Joshua J. Engelsma et al., “Universal 3D Wearable Fingerprint Targets: Advancing Fingerprint Reader Evaluations,” *IEEE Transactions on Information Forensics and Security*, [arXiv:1705.07972 \[cs.CV\]](#) (September 2017).

Forget login, fingerprint, or retinal scan: Your heart is the new identifier

Source: <http://www.homelandsecuritynewswire.com/dr20170926-forget-login-fingerprint-or-retinal-scan-your-heart-is-the-new-identifier>



Sept 27 – Forget fingerprint computer identification or retinal scanning. A University at Buffalo-led team has developed a computer security system using the dimensions of your heart as your identifier. The system uses low-level Doppler radar to measure your heart, and then continually monitors your heart to make sure no one else has stepped in to run your computer.

The technology is described in a paper that the inventors will present at next month's [23rd Annual International Conference on Mobile Computing and Communication](#) (MobiCom) in Utah. The system is a safe and potentially more



CBRNE-TERRORISM NEWSLETTER – October 2017

effective alternative to passwords and other biometric identifiers, they say. It may eventually be used for smartphones and at airport screening barricades.

"We would like to use it for every computer because everyone needs privacy," said Wen Yao Xu, the study's lead author, and an assistant professor in the Department of Computer Science and Engineering in UB's School of Engineering and Applied Sciences.

"Logging-in and logging-out are tedious," he said.

The signal strength of the system's radar "is much less than Wi-Fi," and therefore does not pose any health threat, Xu said.

"We are living in a Wi-Fi surrounding environment every day, and the new system is as safe as those Wi-Fi devices," he said. "The reader is about 5 milliwatts, even less than 1 percent of the radiation from our smartphones."

Buffalo [says](#) that the system needs about eight seconds to scan a heart the first time, and thereafter the monitor can continuously recognize that heart.

The system, which was three years in the making, uses the geometry of the heart, its shape and size, and how it moves to make an identification. "No two people with identical hearts have ever been found," Xu said. And people's hearts do not change shape, unless they suffer from serious heart disease, he said. Heart-based biometrics systems have been used for almost a decade, primarily with electrodes measuring electrocardiogram signals, "but no one has done a non-contact remote device to characterize our hearts' geometry traits for identification," he said.

The new system has several advantages over current biometric tools, like fingerprints and retinal scans, Xu said. First, it is a passive, non-contact device, so users are not bothered with authenticating themselves whenever they log-in. And second, it monitors users constantly. This means the computer will not operate if a different person is in front of it. Therefore, people do not have to remember to log-off when away from their computers.

Xu plans to miniaturize the system and have it installed onto the corners of computer keyboards. The system could also be used for user identification on cell phones. For airport identification, a device could monitor a person up to thirty meters away.

Xu and collaborators will present the paper — "[Cardiac Scan: A Non-contact and Continuous Heart-based User Authentication System](#)" — at MobiCom, which is regarded as the flagship conference in mobile computing. Organized by the Association for Computing Machinery, the conference will be held 16-20 October in Snowbird, Utah.

Social Media is 'First Tool' of 21st-Century Warfare, Lawmaker Says

Source: <http://www.nextgov.com/defense/2017/09/social-media-first-tool-21st-century-warfare-lawmaker-says/141379/>

Sept 28 – One lawmaker believes Russia's use of social media to influence last year's election demonstrated how warfare has moved away from the battlefield and toward the internet.

And the U.S. has been slow to adjust, Sen. Mark Warner, D-Va., said Thursday.

"We may have in America the best 20th-century military that money can buy, but we're increasingly in a world where cyber vulnerability, misinformation and disinformation may be the tools of conflict," Warner said at *The Atlantic's* Washington Ideas fest produced by Atlantic Media, which is *Nextgov's* parent company. "What we may have seen are the first tools of 21st-century disinformation."

As vice chairman of the Senate Intelligence Committee, Warner has helped lead one of the congressional investigations into the Russian meddling in the 2016 election. During a public interview with *The Atlantic's* Steve Clemons, he gave updates on the progress of the investigation and stressed the importance of social media companies helping Congress understand the extent of Russia's involvement. According to Warner, there are three things the committee knows to be true: Russia hacked both political parties and used that information in President Donald Trump's favor; Russia attacked but didn't fully break into the voter registration systems of 21 states; Russia used paid advertising and fake accounts



CBRNE-TERRORISM NEWSLETTER – October 2017

on social media to disseminate misinformation to voters.

The sophistication of Russia's cyber campaign was "unprecedented," he said. It was also cheap. Warner said the amount Moscow spent in total influencing the American, French and Dutch elections was about a quarter the cost of building an F-35 fighter jet.

"If Russia's goal was primarily to sow chaos ... and secondarily elect Mr. Trump, they had a pretty good rate of return," he said.

While Warner said social media companies have helped the investigation thus far, there's still more they can do. For instance, though Facebook linked a troll farm in St. Petersburg, Russia, to many election-related ads, he said the company has so far only sought out bad actors who paid for ads in Russian rubles.

"I think the Russian services maybe know how to use dollars and euros," he said.

Later Thursday, after his committee met with Twitter officials, Warner said the company "showed an enormous lack of understanding" on the seriousness of this issue, [CBS reported](#). He also called the meeting "deeply disappointing." The committee has already asked Twitter, Facebook and Google [to testify before Congress](#) on Nov. 1.

In addition to reluctant social media companies, another barrier the committee has faced is Trump's unwillingness to acknowledge any Russian involvement in the first place, Warner said. Without any point of contact in the White House, it's difficult to lead a governmentwide effort to bolster electoral systems against a future attack.

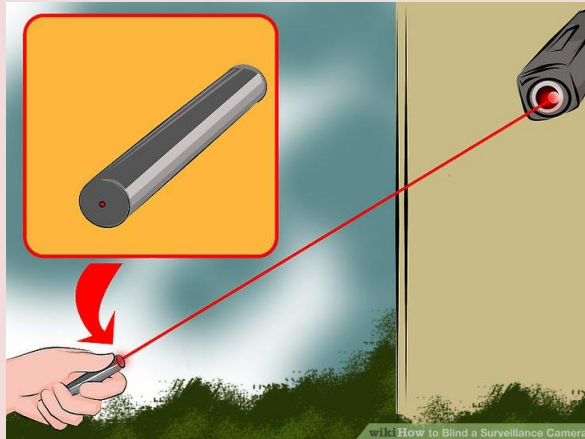
"Our job is to determine whether there was collaboration or collusion, but equally if not more importantly [to determine] how to prevent this from happening again," he said

Using infrared light to hack security cameras

Source: <http://www.homelandsecuritynewswire.com/dr20170929-using-infrared-light-to-hack-security-cameras>

Sept 29 – Ben-Gurion University of the Negev (BGU) researchers have demonstrated that security cameras infected with malware can receive covert signals and leak sensitive information from the very same surveillance devices used to protect facilities.

The method, according to researchers, will work on both professional and home security cameras, and even LED doorbells, which can detect infrared light (IR) that is not visible to the human eye.



In the new [paper](#), the technique the researchers have dubbed "aIR-Jumper" also enables the creation of bidirectional, covert, optical communication between air-gapped internal networks, which are computers isolated and disconnected from the internet that do not allow for remote access to the organization.

AABGU [says](#) that the cyber team led by Dr. Mordechai Guri, head of research and development for BGU's [Cyber Security Research Center](#) (CSRC), shows how IR can be used to create a covert communication channel between malware installed on an internal computer network and an attacker located

hundreds of yards outside or even miles away with direct line of sight. The attacker can use this channel to send commands and receive response messages.

To transmit sensitive information, the attacker uses the camera's IR-emitting LEDs, which are typically used for night vision. The researchers showed how malware can control the intensity of the IR to communicate with a remote attacker that can receive signals with a simple camera without detection. Then the attacker can record and decode these signals to leak sensitive information.

The researchers shot two videos to highlight their technique. The [first video](#) shows an attacker hundreds of yards away sending infrared signals to a camera. The [second video](#) shows the camera infected with malware responding to covert signals by exfiltration data, including passwords.



CBRNE-TERRORISM NEWSLETTER – October 2017

According to Dr. Guri, “Security cameras are unique in that they have ‘one leg’ inside the organization, connected to the internal networks for security purposes, and ‘the other leg’ outside the organization, aimed specifically at a nearby public space, providing very convenient optical access from various directions and angles.”

Attackers can also use this novel covert channel to communicate with malware inside the organization. An attacker can infiltrate data, transmitting hidden signals via the camera’s IR LEDs. Binary data such as command and control (C&C) messages can be hidden in the video stream, recorded by the surveillance cameras, and intercepted and decoded by the malware residing in the network.

“Theoretically, you can send an infrared command to tell a high-security system to simply unlock the gate or front door to your house,” Guri says.

— Read more in Mordechai Guri et al., “aIR-Jumper: Covert Air-Gap Exfiltration/Infiltration via Security Cameras & Infrared (IR),” [arXiv:1709.05742 \[cs CR\]](https://arxiv.org/abs/1709.05742) (18 September 2017).

Is your smart coffee maker a national security risk?

Source: <http://www.dailymail.co.uk/sciencetech/article-4881798/Is-smart-coffee-maker-national-security-risk.html>

Sept 13 – From refrigerators to baby monitors, all kinds of smart devices are connected to the Internet of Things.

But now, the federal government is worried that some connected devices could be a threat to national security.

A bi-partisan group of senators is sponsoring legislation to make the Internet of Things safer - devices with computer chips and sensors that are connected to the internet.

Colorado’s US Senator Cory Gardner, who is part of the bi-partisan group, told *CBS Denver* that these devices could be used as weapons of mass destruction.

‘The federal government orders billions of dollars worth of Internet of Things devices each and every year,’ said Senator Gardner.



Pictured left is Griffin Technology's Bluetooth-enabled coffee maker, and right its toaster, which remembers your preferences

'These are things that can be hacked into.

'You can try to control systems, instruments with them.



CBRNE-TERRORISM NEWSLETTER – October 2017

'You can certainly read what people are doing and maybe even eavesdrop on a conversation people are having.'

Last year, for example, hackers shut down major websites such as Twitter and Spotify, and 500,000 items were potentially at risk of being activated without their owners' knowledge, with everything from baby monitors, DVR's, security cameras and other gadgets turned into cyber weapons.

A recent [study](#) by researchers at the University of Princeton found that details of your private habits within your own home could be sold on to advertisers by broadband providers.

Information transmitted by products ranging from home security cameras, toasters and sleep monitors could be sold to third parties to help them target their products.

The researchers set up their own test smart home, fitted with seven Internet of Things (IoT) devices.

They hoped to examine the kind of data they might reveal about their users, by looking at metadata.

This includes how and when someone accesses their internet connection, but not what they have sent and received.

This information is relatively unprotected and can reveal private information about our personal habits.

This could range from when we access an internet connected baby monitor to our use of smart sex toys.

The Princeton team found that Internet Service Providers could identify four of the devices, including an Amazon Echo, by characteristic features of how they connect to the internet alone.

Senator Gardner, who is also Chair of the Senate Cybersecurity Caucus, is sponsoring a bill that would require internet-connected devices bought by the government to meet certain security standards - for example through measures such as firewalling off information and making sure that there isn't a hardcoded password from a factory that someone has access to.

According to Senator Gardner, many of these devices are imported from other countries and are not secure, making them vulnerable doors into governments that can be used by criminals or other nations.

'We're facing kind of a brave new world when it comes to these things and we need to be prepared from a policy standpoint to address it,' said Senator Gardner.

Although this legislation only applies to devices purchased by the government, Senator Gardner hopes the changes will be applied to devices sold in the private sector.



Pictured left is Griffin Technology's Bluetooth-enabled coffee maker, and right its toaster, which remembers your preferences

BIZARRE HOME DEVICES THAT ARE CONNECTED TO THE INTERNET

From refrigerators to baby monitors, all kinds of smart devices are connected to the Internet of Things. But now, the federal government is worried that some connected devices are could be a threat to national security.

Just some of the devices that are connected to the internet include:

- Smalt: A smart salt shaker with built-in speakers
- Mimo: A connected onesie that monitors a baby's heart rate and oxygen levels



CBRNE-TERRORISM NEWSLETTER – October 2017

- Connected mirror: Giffin's Connected Mirror won't just show you your reflection, the smart device presents time, weather and status messages from other Griffin Home products.
- Vessyl: An internet connected cup that tells you what's inside your drink and it's nutritional content.
- FitBark: A dog collar that works as an activity tracker for dogs.
- Loon Cup: A smart menstrual cup which helps women track the flow of their periods, alerting your phone when it needs to be emptied.
- Lixil Satis Integrated toilet: A toilet that can be controlled by a companion app, which lets you track on a calendar when you've gone to the bathroom.
- Bluesmart's bluetooth luggage: A luggage with mobile connection and built-in scale, and a digital lock that can be controlled by an Apple Watch.

Internet Organised Crime Threat Assessment (IOCTA) 2017

Source: <https://www.europol.europa.eu/activities-services/main-reports/internet-organised-crime-threat-assessment-iocta-2017>



The 2017 Internet Organised Crime Threat Assessment (IOCTA) reports how cybercrime continues to grow and evolve. While many aspects of cybercrime are firmly established, other areas of cybercrime have witnessed a striking upsurge in activity, including attacks on an unprecedented scale, as cybercrime continues to take new forms and new directions. A handful of cyber-attacks have caused widespread public concern but only represented a small sample of the wide array of cyber threats now faced.

►► Read the full report at: [Internet Organised Crime Threat Assessment 2017](https://www.europol.europa.eu/activities-services/main-reports/internet-organised-crime-threat-assessment-iocta-2017)

Cyber-security threat to UK 'as serious as terrorism'

Source: <http://www.bbc.com/news/uk-41547478>

Oct 09 – **Keeping the UK safe from cyber-attacks is now as important as fighting terrorism,** the head of the intelligence monitoring service GCHQ has said.

Jeremy Fleming said increased funding for GCHQ was being spent on making it a "cyber-organisation" as much as an intelligence and counter-terrorism one.

It comes after the NHS and parliament suffered cyber-attacks this year.

Mr Fleming said there had been nearly 600 "significant" cyber-attacks needing a national response in the last year.

'Deeply challenging'

Writing in the Daily Telegraph, the ex-deputy director of MI5, who became GCHQ director in March, said the UK's adversaries were "quick to spot new ways of doing us harm".

"We see that in the way terrorists are constantly changing their weapons, or states are using their full range of tools to steal secrets, gain influence and attack our economy".

But he said until the UK's National Cyber Security Centre (NCSC) was set up last year, GCHQ's work



CBRNE-TERRORISM NEWSLETTER – October 2017

on cyber-security "too often felt like the poor relation".

The NCSC now has a "world-leading programme to reduce the incidence and impact of cyber-attacks without users even noticing," he added.

It now works with private firms, schools and universities as well as the media, as part of its cyber-security role.

That can "feel deeply challenging" for the secretive Cheltenham-based agency, which is used to working "in the shadows", he added.

Digital homeland

However, he said: "If GCHQ is to continue to help keep the country safe, then protecting the digital homeland - keeping our citizens safe and free online - must become and remain as much

part of our mission as our global intelligence reach and our round-the-clock efforts against terrorism."

In May, NHS services across England and Scotland were hit by a large-scale cyber-attack that disrupted hospital and GP appointments.

The incident was part of an untargeted wider attack affecting organisations globally.

And in June, up to 90 email accounts were compromised during the [cyber-attack on Parliament](#).

Last week, NCSC head Ciaran Martin said 1,131 cyber-attacks were reported in the centre's first year. Of those, 590 were classed as significant and more than 30 were assessed as serious enough to require a cross-government response.

How future Olympic Games might be hacked

Source: <http://www.localnews8.com/sports/how-future-olympic-games-might-be-hacked/636069213>

Oct 11 – A hacked result could mean the difference between an Olympic gold medal and an athlete watching the award ceremony from the sidelines.

As sporting events increasingly go digital -- from the stadium systems to scorekeeping -- experts warn those systems can be hacked.

The Berkeley Center for Long-Term Cybersecurity released new research on Tuesday that says hackers could disrupt everything from ticketing to announcement systems in an effort to cause chaos or win medals at massive sporting events.

The study focused on the Olympic Games over the next 10 to 15 years. The research is backed in part by the Los Angeles Organizing Committee for the Olympic and Paralympic Games 2028.

The California city is hosting the summer Olympics in just over a decade.

Current cybersecurity efforts are still largely focused on areas like protecting websites or email accounts. Betsy Cooper, executive director of the Berkeley Center for Long-Term Cybersecurity and the paper's lead author, said people should consider a broader range of threats.

"The worst thing that most people think about happening is 'What if the website goes down?'" she said. "But just as we've seen in the 2016 election, you have to be really creative in thinking about the types of implications that

someone [may] impose on a major sporting event."

The report lists eight key areas of risk for Olympic meddling, including hacks on photo or video replays, athlete care, transportation, and panic-inducing actions. In the not-too-distant future, the report says, the world might see a headline like this one: "Austrian Swimmer Allegedly Hired Hacker to Gain Access to Competitors' Email."

The Olympics is ostensibly a neutral platform but is often politicized or manipulated. During the Cold War, attention focused largely on the the U.S. and Russia competition. In 1972, a group of Palestinian terrorists kidnapped and eventually killed 11 Israeli Olympic team members at the Munich Olympics. In 2016, the former head of Russia's anti-doping laboratory exposed a state-run drug program designed to make Russian athletes win at the 2014 Sochi Olympics.

Sports is already a focus of hackers. Last year, Russian hackers leaked medical data related to 25 Olympic athletes. Organizations and websites affiliated with the Rio Olympics experienced distributed denial of service (DDoS) attacks in the summer of 2016. Hackers targeted the 2014 World Cup in Brazil. The hacker group Anonymous launched a DDoS attack on the Formula 1 website in 2012.



CBRNE-TERRORISM NEWSLETTER – October 2017

Machines monitor a lot of sporting activity, and in one sport, computerized decision making is the norm. A system called Hawk-Eye is used in major sports like tennis and lets players challenge whether the ball was in or out. The digital technology's decision overrules the human umpire.

"If somebody could get into the Hawk-Eye system and manipulate the way it makes decisions, it could actually affect the outcome of the sport," Cooper said. "As we include more digital technologies into sports and use them to detect false starts and to measure the amplitude of a jump, we also incorporate new vectors of possible risk."

Cooper says attackers could also use hacks to cause physical harm. For example, a terrorist hacker could put messages on a scoreboard that cause people to panic and rush out of the stadium.

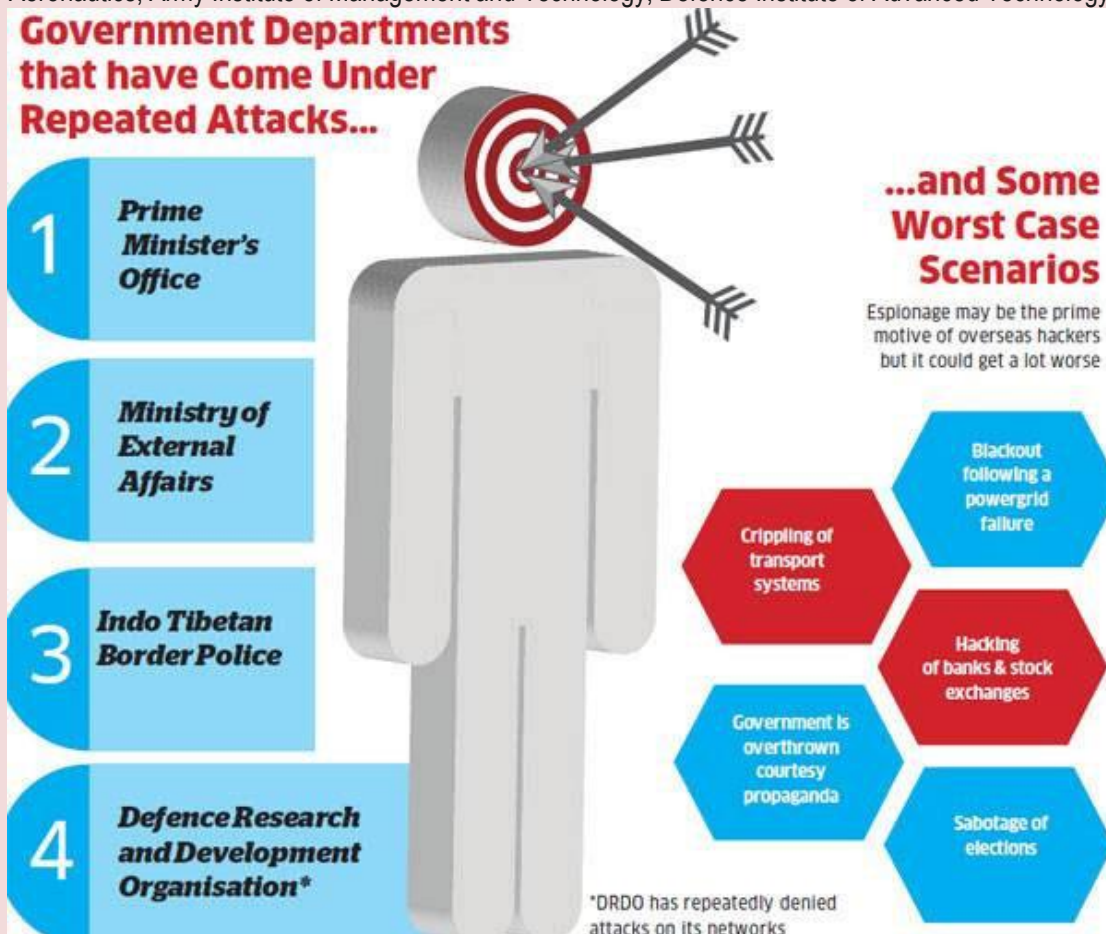
Cooper hopes the research helps people better understand the potential risks of adding digital technologies to sports without weighing the consequences.

"In events like sports, like elections, like all sorts of systems in our world, we need to start thinking about cybersecurity as something everyone has a role to play in, not just the IT manager," she said.

India is quietly preparing a cyber warfare unit to fight a new kind of enemy

Source: <https://economictimes.indiatimes.com/news/defence/india-is-quietly-preparing-a-cyber-warfare-unit-to-fight-a-new-kind-of-enemy/articleshow/61141277.cms>

Oct 19 – Recently, Pakistani [hackers](#) compromised 10 Indian websites which included National Aeronautics, Army Institute of Management and Technology, Defence Institute of Advanced Technology,



Army Institute of Management, and the Board of Research in Nuclear Sciences.

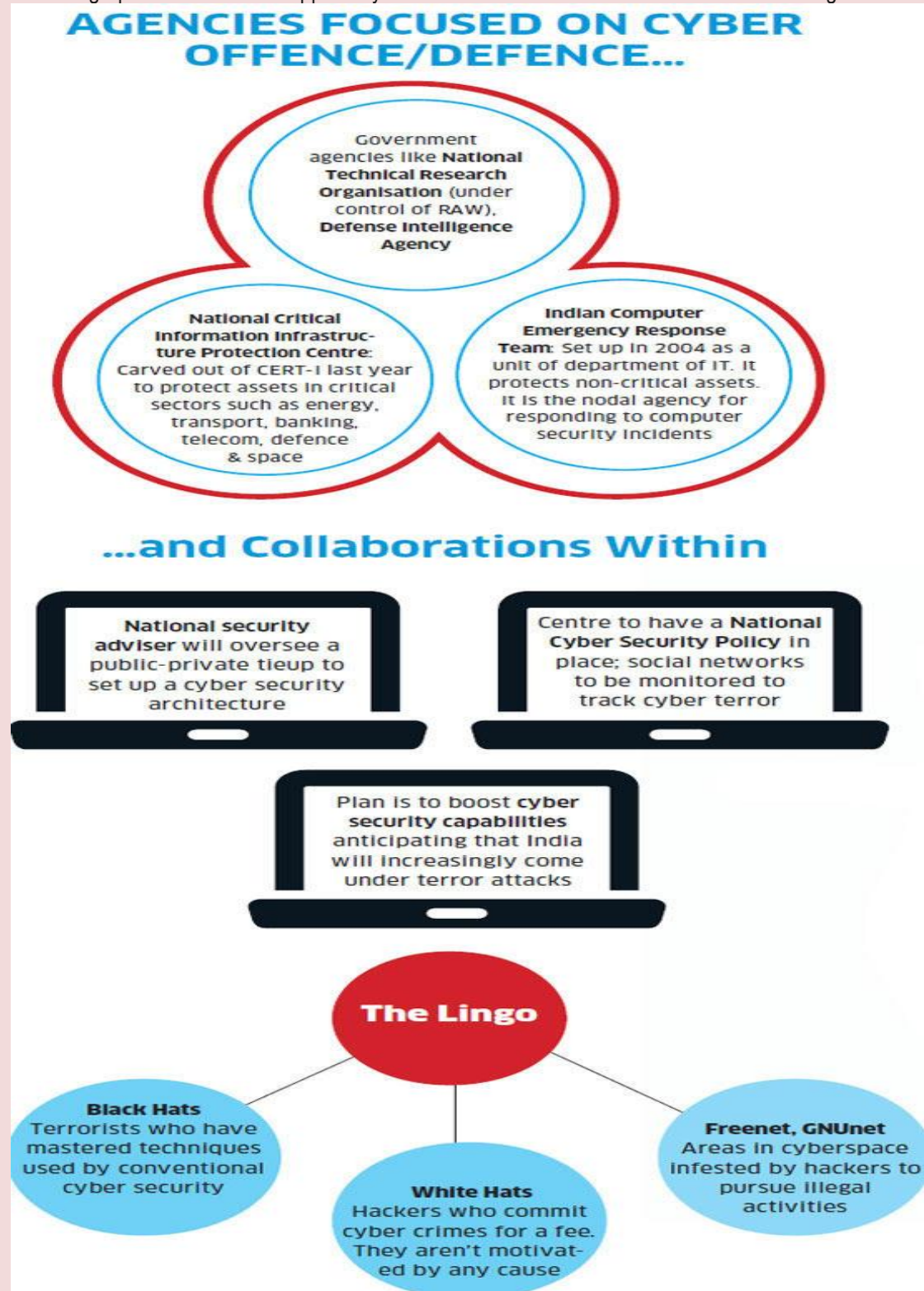


CBRNE-TERRORISM NEWSLETTER – October 2017

The hacker group — [Pakistan](#) Haxor Crew — claimed the action was to avenge the defacement of the Pakistan Railways website by an Indian hacker and to show solidarity with Kashmiris.

Last year, reports emerged in Australia that the entire design plans that reveal the capability of India's Scorpene submarine fleet were leaked.

The design plans were leaked apparently from French manufacturer DCNS that is the designer of the



system.

According to reports, more than 22,000 pages of plans had been leaked.



CBRNE-TERRORISM NEWSLETTER – October 2017

An IIT Kanpur study shared with Parliament's Committee on Finance this year said attacks from the 'Equation group' — which a WikiLeaks reports said was a clandestine CIA and NSA programme — infected India's telecom and military sectors and research institutes.

The government is finally reacting to the threat with a plan to create a new tri-service agency for cyber warfare. The Defence Cyber Agency will work in coordination with the National Cyber Security Advisor. It will have more than 1,000 experts who will be distributed into a number of formations of the Army, Navy and IAF.

According to reports, the new Defence Cyber Agency will have both offensive and defensive capacity. The Defence Cyber Agency is seen as a precursor of a cyber command. After reports that Russia meddled in the US elections by hacking machines and creating propaganda on the internet and the recent ransomware and other cyber attacks being attributed to North Korea, cyber warfare is gaining importance.

According to experts, North Koreans have developed an advanced cyber program that steals hundreds of millions of dollars and can trigger global havoc.

Minister of State for Home Kiren Rijiju admitted last month that there was a huge gap in India's capability and capacity when it came to cyber warfare and it was imperative to narrow down this difference to discourage cyber attackers.

[China](#) has already developed strong cyber warfare capacity. The next war may well have to be fought on the internet where a country's vital networks and infrastructure would be on target that will create bigger disruption than actual wars.

Equally important is cyber propaganda. During the Doklam conflict, China tried its best to unleash cyber propaganda on India and indulged in complex psy-ops.

A Defence Cyber Agency could be the first step the government plans to for critical infrastructure and military networks that are increasingly becoming dependent on the Internet, thus increasing vulnerabilities.





EMERGENCY RESPONSE





Technique spots warning signs of extreme events

Source: <http://news.mit.edu/2017/technique-spots-warning-signs-climate-aircraft-oceans-0922>

Sept 22 – Many extreme events — from a rogue wave that rises up from calm waters, to an instability inside a gas turbine, to the sudden extinction of a previously hardy wildlife species — seem to occur without warning. It's often impossible to predict when such bursts of instability will strike, particularly in systems with a complex and ever-changing mix of players and pieces.

Now engineers at MIT have devised a framework for identifying key patterns that precede an extreme event. The framework can be applied to a wide range of complicated, multidimensional systems to pick out the warning signs that are most likely to occur in the real world.

"Currently there is no method to explain when these extreme events occur," says **Themistoklis Sapsis, associate professor of mechanical and ocean engineering at MIT.**

"We have applied this framework to turbulent fluid flows, which are the Holy Grail of extreme events. They're encountered in climate dynamics in the form of extreme rainfall, in engineering fluid flows such as stresses around an airfoil, and acoustic instabilities inside gas turbines. If we can predict the occurrence of these extreme events, hopefully we can apply some control strategies to avoid them."

Sapsis and MIT postdoc Mohammad Farazmand have published their results today in the journal *Science Advances*.

Looking past exotic warnings

In predicting extreme events in complex systems, scientists have typically attempted to solve sets of dynamical equations — incredibly complex mathematical formulas that, once solved, can predict the state of a complex system over time.

Researchers can plug into such equations a set of initial conditions, or values for certain variables, and solve the equations under those conditions. If the result yields a state that is considered an extreme event in the system, scientists can conclude that those initial conditions must be a precursor, or warning sign. Dynamical equations are formulated based on a system's underlying physics. But Sapsis says that the physics governing many complex systems are often not well-understood and they

contain important model errors. Relying on these equations to predict the state of such systems would therefore be unrealistic.

Even in systems where the physics are well-characterized, he says there is a huge number of initial conditions one could plug into associated equations, to yield an equally huge number of possible outcomes. What's more, the equations, based on theory, might successfully identify an enormous number of precursors for extreme events, but those precursors, or initial states, might not all occur in the real world.

"If we just blindly take the equations and start looking for initial states that evolve to extreme events, there is a high probability we will end up with initial states that are very exotic, meaning they will never ever occur for any practical situation," Sapsis says. "So equations contain more information than we really need."

Aside from equations, scientists have also looked through available data on real-world systems to pick out characteristic warning patterns. But by their nature, extreme events occur only rarely, and Sapsis says if one were to rely solely on data, they would need an enormous amount of data, over a long period of time, to be able to identify precursors with any certainty.

Searching for hotspots

The researchers instead developed a general framework, in the form of a computer algorithm, that combines both equations and available data to identify the precursors of extreme events that are most likely to occur in the real world.

"We are looking at the equations for possible states that have very high growth rates and become extreme events, but they are also consistent with data, telling us whether this state has any likelihood of occurring, or if it's something so exotic that, yes, it will lead to an extreme event, but the probability of it occurring is basically zero," Sapsis says.

In this way, the framework acts as a sort of sieve, capturing only those precursors that one would actually see in a real-world system.

Sapsis and Farazmand tested their approach on a model of turbulent fluid flow — a prototype system of fluid dynamics that describes a chaotic fluid, such as a plume of cigarette smoke, the



CBRNE-TERRORISM NEWSLETTER – October 2017

airflow around a jet engine, ocean and atmospheric circulation, and even the flow of blood through heart valves and arteries.

“We used the equations describing the system, as well as some basic properties of the system, expressed through data obtained from a small number of numerical simulations, and we came up with precursors which are characteristic signals, telling us before the extreme event starts to develop, that there is something coming up,” Sapsis explains.

They then performed a simulation of a turbulent fluid flow and looked for the precursors that their method predicted. They found the precursors developed into extreme events between 75 and 99 percent of the time, depending on the complexity of the fluid flow they were simulating.

Sapsis says the framework is generalizable enough to apply to a wide range of systems in which extreme events may occur. He plans to apply the technique to scenarios in which fluid flows against a boundary or wall. Examples, he says, are air flows around jet planes, and ocean currents against oil risers.

“This happens in random places around the world, and the question is being able to predict where these vortices or hotspots of extreme events will occur,” Sapsis says. “If you can predict where these things occur, maybe you can develop some control techniques to suppress them.”

This research was supported, in part, by the Office of Naval Research, the Air Force Office of Scientific Research, and the Army Research Office.

Hurricane loss model estimates damage caused by Hurricane Irma at \$19 billion

Source: <http://www.homelandsecuritynewswire.com/dr20170928-hurricane-loss-model-estimates-damage-caused-by-hurricane-irma-at-19-billion>

Sept 28 – A team of researchers estimates that Hurricane Irma caused \$19.4 billion in wind-related losses to Florida residents alone. The data does not cover flood losses. **Of that total, \$6.3 billion will be paid by insurance companies.** As a result, roughly two-thirds of the losses will be borne by homeowners.

AI, citizen science, disaster response combine to help Hurricane Irma's victims

Source: <http://www.homelandsecuritynewswire.com/dr20170928-ai-citizen-science-disaster-response-combine-to-help-hurricane-irma-s-victims>

Sept 28 – **A highly unusual collaboration between information engineers at Oxford, the Zooniverse citizen science platform, and international disaster response organization Rescue Global is enabling a rapid and effective response to Hurricane Irma.**



CBRNE-TERRORISM NEWSLETTER – October 2017

The project draws on the power of the Zooniverse, the world's largest and most popular people-powered research platform, to work with volunteers and crowd source the data needed to understand Irma's path of destruction and the damage caused. Combining these insights with detailed artificial intelligence will support rescue relief organizations to understand the scale of the crisis, and deliver aid to those worst affected as soon as possible.

Irma is now judged to be the most powerful Atlantic storm in a decade, breaking previous extreme weather records and causing widespread destruction and death across the Caribbean. Tens of thousands of people have been displaced or made homeless, and well over a million are who lost critical services such as water and electricity. The disaster posed huge challenges for crisis response teams, who needed to assess as quickly as possible the extent of the destruction on islands spread over thousands of square miles, and ensure that the right aid gets to those in most need in the safest and most efficient way.

Oxford [notes](#) that in the immediate aftermath of Irma, Oxford researchers have been working round the clock in partnership with Rescue Global, a respected international crisis response charity, to help address

this problem. The results have already supported Rescue Global to get aid delivered to some of the areas worst affected by Irma.

On 12 September the Zooniverse, which was founded by Oxford researchers, relaunched its Planetary Response Network (PRN). First trialed in the days following the Nepal earthquake of April 2015, the PRN aims to mobilize a "crowd" to assist in a live disaster that is still unfolding. Before, during, and in the days that followed Irma, thousands of volunteers from around the world joined the effort. Their role is to analyze "before" and "after" satellite images of the



islands hit by Irma and identify features such as damaged buildings, flooding, blocked roads or new temporary settlements which indicate that people are homeless.

Rebekah Yore, Operations Manager at Rescue Global, commented: "By the morning of Friday 15th September, we were told by the Zooniverse team that roughly 300,000 classifications from 7,500 people had taken place through the platform. This extraordinary effort is the equivalent to the output of one person working full-time for just over a year, or that same person working 24/7 without breaks for around three months. And the number of volunteers and classifications are increasing daily. This input is already having a direct effect on the ground, helping to provide situational awareness for all deployed teams."

The sheer volume of images would take an individual months to sort through, but can be analyzed in a matter of hours by the "crowd." Because the images are often of poor quality, human observers are much better placed to perform this part of the task than computers.

For the next step, however, computers are essential, and Oxford engineering researchers have developed a suite of sophisticated artificial intelligence tools which can process the resulting data. Machine learning approaches quickly reconcile inconsistent responses, aggregate the data and integrate information derived from other crowd-sourced mapping materials, such as the Humanitarian Open Street Maps and Tomnod. This approach generates the best information possible to inform relief efforts. This analysis enables the team to build impact 'heat maps' that identify the areas in need of urgent assistance. Oxford has considerable expertise in this area: the tools have been refined over several years and were previously used to assist Rescue Global in its response to the 2015 Nepal and 2016 Ecuador earthquakes.

The "heat maps" enable Rescue Global to decide where to send its own small reconnaissance planes to conduct detailed aerial assessments, and to share critical information with a multitude of governmental and humanitarian partners [see <http://www.rescueglobal.org/hurricane-irma>]. Working closely with Airlink, which flew in aid to a central location, Rescue Global has been using information gathered through the Zooniverse platform and its own needs assessments to coordinate the onward delivery of aid through a network of boats and planes, ensuring that it gets to those who need it most.



Oxford says that this new technology offers an evidence-based, rational approach to disaster management. Through collaboration with crisis responders like Rescue Global, Oxford researchers are making a unique and significant difference to victims of Hurricane Irma.

Dr. Steven Reece, Machine Learning Research Fellow and mapping lead at Oxford University, said: “As always we are extremely grateful to our friends in the satellite industry for providing data and, of course, the crowd for their amazing work interpreting the imagery so quickly. This has been a sustained campaign and we’ve now produced heat maps for all the Virgin Islands. With Hurricane Maria increasing in strength and bearing down on the same area, we will have a lot more work ahead of us.”

Mass casualty incidents and the overlap between trauma systems and hospital disaster preparedness

Source: <http://www.homelandsecuritynewswire.com/dr20171004-mass-casualty-incidents-and-the-overlap-between-trauma-systems-and-hospital-disaster-preparedness>

Oct 04 – The horrific mass shooting in Las Vegas on 1 October 2017 has resulted in nearly sixty deaths and more than 500 injuries at the time of this writing. The injured have been transported to a number of hospitals around Las Vegas and have overwhelmed some of the hospitals closest to the scene. A number of the injured are in critical condition and hence the death toll is likely to rise. Among other issues, this tragedy illustrates the overlap between trauma systems and hospital disaster preparedness.

Eric Toner, MD, [writes](#) in the *Bifurcated Needle* that a single patient with a gunshot wound (GSW) to a vital body part (e.g., head, chest, abdomen, or major artery) will stress a typical community hospital. Most community hospitals do not routinely treat these kinds of patients because trauma systems have been organized across the country over the last 50-60 years. Trauma systems consist of hospitals that have been certified as having varying levels of expertise and resources for treating trauma victims. Level I trauma centers are held to the highest standard, Level III to the lowest. University Medical Center is the only Level I trauma center in Nevada, and [reports indicate that at least 30 critical patients](#) were treated in its trauma center and more than 100 non-critical patients in the emergency department. Sunrise Hospital, a Level II trauma center and the closest trauma center to the shooting, [reports having treated 180 patients](#) and operated on approximately 30.

Today, Emergency Medical Services (EMS) ambulances will usually transport severely injured patients to accredited trauma centers, which are typically part of large academic medical centers. Toner writes that as a result, **community hospitals rarely treat gunshot**

wounds anymore except for the occasional “walk-in” minor gunshot victim.

Before the creation of trauma centers in the 1960s and 1970s the situation was different: patients with severe traumatic injuries, including GSWs, would be taken to the closest hospital where general surgeons with varying degrees of trauma training and experience would treat them. The patient outcomes were often less than optimal.

Level 1 trauma centers have round-the-clock in-house coverage by specially trained trauma surgeons, surgical subspecialists (e.g., thoracic, cardiovascular, neuro), and anesthesiologists. In addition, they have specialized equipment—such as cardiac bypass—not often found in community hospitals. With the advent of the specialized trauma centers, patient outcomes have greatly improved but this progress has come at a price: community hospitals’ trauma capabilities have atrophied because they no longer routinely see severe trauma patients. A severe trauma patient who does somehow present to a community hospital emergency department these days is typically stabilized and transferred to a trauma center as quickly as possible. On a routine day-to-day basis, this benefits the patients, but in a large-scale trauma disaster like a mass shooting this centralization of trauma care limits a community’s surge capacity for trauma in a disaster.

While all hospitals must have disaster plans and practice them twice a year, no hospital can handle a large-scale disaster on its own—especially a complex mass casualty event.

Because of this challenge, hospital disaster preparedness and response is increasingly organized around collaboration among different hospitals and



CBRNE-TERRORISM NEWSLETTER – October 2017

between hospital and EMS, emergency management, and public health agencies. This has given rise to healthcare coalitions across the country.

Toner notes that complex mass casualty events of all types (e.g., chemical, biological, radiological) require highly specialized care that is only found in large academic medical centers—the same hospitals that are the Level 1 trauma centers. **For the most part, community hospitals do not have the resources, depth of staff, or expertise needed for these types of events.** But even the largest trauma centers can be overwhelmed by a very large-scale mass disaster. “It is

therefore important that trauma centers be integrated with the other hospitals in the community in a well-coordinated system that delivers the right care to the right patient in the right place—the more severe injuries to the trauma centers and the less severe to other facilities. For this to work well, it must be planned and practiced. In my view, this is best done through the emerging healthcare coalitions. As the disaster preparedness and response system continues to develop in the United States, it should be integrated with the existing trauma system with large academic medical centers being at the hub of both systems,” Toner concludes.

Three Storms Demonstrate Five Forms of Flooding

By John Englander

Source: <https://www.domesticpreparedness.com/preparedness/three-storms-demonstrate-five-forms-of-flooding/>

Oct 11 – **Flooding results from three primary forces: rainfall, coastal storm surge, and rising sea level, made even worse with by runoff and extreme tides.** Recently, hurricanes Harvey, Irma, and Maria showcased the new environmental conditions the world faces as well as the devastating damage that can occur when any combination of these flood types converges on a built community constructed without adequately addressing the increasing threats.

Category 4 Hurricane Harvey rapidly developed within approximately 36 hours in the Gulf. As Harvey made landfall on 25 August 2017, huge waves struck the coastline, storm surge rose even higher in the bays, and a 40-inch deluge of rain caused massive flooding. Flooding worsened over the next few days on the Texas coast as the storm moved slowly eastward toward Houston and Galveston. The shallow warm waters of the northern Gulf and the extensive bays behind the barrier islands nourished and sustained the downpour. Two weeks later, Category 5 Hurricane Irma, with sustained record winds of 185 miles per hour, killed dozens, destroyed nearly all structures on some Caribbean islands, and then threatened the Florida coasts. Less than two weeks after Irma, Category 4 Hurricane Maria, with sustained winds of 155 mph, struck the island of Puerto Rico, causing widespread damage across all of its communities.

Reasons for Unusual & Unpredictable Storms

One reason for these harder to predict, unusual storms is that 93% of the extra heat being trapped in the atmosphere by increased greenhouse gases is being stored in the ocean. The Gulf of Mexico is a relatively shallow isolated body of water that is [particularly susceptible to warming](#). In simple terms, that is why Harvey hit with minimal notice and produced flooding that exceeded models. Higher heat levels can even alter ocean currents like the Gulf Stream and atmospheric currents like the Jet Stream, causing unpredictable storms and weather systems, outside the historical record. Subtle temperature changes in the deep ocean further complicate the picture obtained from the easily measured sea surface temperatures.

Unusual weather patterns, including storms and record-breaking rain, are related to the warmer ocean. Although the usual weather forecasts are becoming extraordinarily accurate, many big pattern phenomena like hurricanes and *el Niños* are getting harder to accurately forecast. Warmer temperatures are melting vast areas of glaciers and polar ice sheets that will raise global sea level far into the future. Since ice melts at an exact temperature, sea level is a good proxy for global average temperature over centuries and millennia. The natural climate cycles are perhaps best exemplified by the ice ages. [Sea level reaching levels unknown](#) for more than 100,000 years add a new dimension to the challenge posed by flooding.





Texas National Guard and the U.S. Military aid victims in the aftermath of Hurricane Harvey in Houston (Source: Defense.gov, 27 August 2017).

Five Forms of Flooding

Solutions to the extreme flooding from recent hurricanes are complex, with three primary flooding forces to consider: storms pushing water in from the sea; record rainfall; and rising sea level and two secondary level forces, runoff and extreme tides. These forces operate somewhat independently, but can combine for a devastating effect. Communities are caught in the triangulation: deluge from above; base sea level rising from below; and waves and storm surge approaching laterally from the coast. In order to design viable communities for the future, it is imperative to understand the dynamics of each of the five flooding forms and why the design solutions can be quite different.

- ◆ **Rainfall** – Harvey demonstrated record levels of rain, more than a foot in a few hours. The warmer ocean temperature means more water evaporates, putting water molecules and heat energy into the atmosphere in much higher volumes than “normal,” which must come down as more precipitation.
- ◆ **Runoff** – Extreme rainfall can trigger the related problem of runoff, causing far greater flooding as water flows to lower elevations in a city, down a valley, or into a stream/river possibly overflowing river banks hundreds of miles away. As the ground saturates and can no longer absorb the rainfall, flooding can suddenly worsen. (Adding to the problem, Houston does not have zoning restrictions to allocate development density and plans for adequate drainage at the scale of a master plan.)
- ◆ **Storm surge** – Aside from the wind and rain, the special threats from a major storm are the huge waves at the coast and the storm surge. The cyclone force of a hurricane essentially “sucks” a huge quantity of seawater with its low pressure and pushes a virtual giant wall of water as it moves. That water surge creates a special problem when it is pushed into a confined, or even semi-confined space, such as a bay, harbor, or intracoastal waterway and “piles up” to much greater heights. In Texas during Harvey, this occurred as the large water volume moved behind the coastal barrier islands, and into the bays, canals, estuaries, and harbors from Corpus Christi to Houston/Galveston.
- ◆ **Sea level** – Sea level has just started to rise. The primary driver is ice melt on land (i.e., the glaciers and ice sheets largely on Alaska, Greenland, and Antarctica). Rising sea level has been modest to date, but will soon start to rise at an increasing rate, in fact,



CBRNE-TERRORISM NEWSLETTER – October 2017

almost certainly an exponential one (for further explanation, read [“Beware the Doubling Time for Rising Seas”](#)). The key difference with sea level rise from the other two primary flood factors is that it is slow and stealthy. It is often overlooked as communities focus on the big events of storms and heavy rainfall. Yet, as sea level rises over the coming decades, it will essentially cause permanent change to coastal areas around the world. The effects go through marshlands and up tidal waterways rather far inland.

- ◆ **“King Tides”** – Following the pull of the moon and other planets, the oceans change height on a regular tidal cycle, varying somewhat by location. The extreme high tides are often referred to as “king tides” and can be predicted to the minute for various locations. Over the last few decades as sea level rise accelerates, the height and extent of the king tides is getting noticeably greater. From San Francisco Bay to Annapolis and from Vancouver to Miami, this routine flooding is becoming more than a nuisance, even though it recedes in hours. It is driven by and is the harbinger of creeping higher *permanent* sea level. (“Permanent” here in the sense that sea level is unlikely to go down for millennia.) At the convergence of these five flooding forms, even engineers, architects, and planners find themselves challenged in terms of how to plan for new flooding extremes, where the past no longer easily predicts the future. In Texas and Louisiana, Hurricane Harvey illustrated the challenge of designing viable solutions for the rapidly changing environment. Drainage systems were overwhelmed. Pavement, concrete, and buildings all stopped water from absorbing into the ground.

Possible Solutions

The lessons of these three recent storms are profound and powerful. Specifically, Houston needs to implement good zoning, building codes, and storm water management. Bayous are not something to be paved over with urban sprawl, without consequence. Puerto Rico not only needs to rebuild with new building codes, this should be the opportunity to redesign its power system from the ground up. This is also a good opportunity to design a large-scale system of solar, wind, microgrids, and batteries using the latest technology. Despite a potential catastrophic scenario, Florida mostly escaped disaster this time, but may not fare as well with the next storm, and certainly not with sea level rise.



Solutions for rainfall and runoff require more robust drainage systems, including retention ponds, larger storm culverts, pumps, and areas to absorb the water. Storm surge from the sea, though, is entirely different. One proposed solution to deflect the storm surge at Galveston, at the mouth of the Houston Ship Channel is an [\\$11 billion storm barrier](#). However, structures designed to stop waves and storm surge would not stop slowly rising sea level. A dam or water-tight barrier to protect against rising sea level would need to accommodate shipping traffic efficiently, posing a different design challenge. Also, gates or barriers do nothing to solve the problem of record



CBRNE-TERRORISM NEWSLETTER – October 2017

rainfall and runoff. In fact, many storm surge barriers or sea walls could actually act to retain the flooding from rainfall, making the problem even worse.

With extreme rainfall, the solution to prevent flooding has to be drainage systems, elevating buildings, or even relocating low-lying neighborhoods. Realistic solutions should also include revisions to building codes, zoning, and restoration of wetlands. The key is to design for and adapt to this new reality, recognizing the very different flooding forces.

Though a somewhat separate issue, there needs to be a slowing of carbon dioxide and other greenhouse gas releases that are trapping heat and warming the planet. That means instituting policies to reduce reliance on fossil fuels and reduce the level of greenhouse gases that correlate with the warming temperatures. Slowing the warming process and adapting to changing climates need to be done simultaneously and aggressively.

Adapting communities for the five different forms of flooding will not be easy. The effects are very different, with storms, rainfall, runoff, and king tides causing short-term flooding and sea level rise potentially putting property underwater permanently. Rising sea level is a special problem, as it slowly increases the water levels from other short-lived flooding factors. However, understanding these different aspects clearly can facilitate designs for greater resilience for all of them.



Flooding comes in different forms that can require different solutions. This Fort Lauderdale street with trucks in the foreground and boats in the background illustrates how “king tides” now routinely flood streets. Even a “no wake” sign typically aimed at boats, is intended here to get cars to drive slowly, to minimize salt water waves in the neighborhood (*Source: Bob Gremillion, January 2017*).

A New Era of Water Challenges

As long as the planet continues warming with increases in carbon dioxide and other greenhouse gases, sea levels will rise, storm surges will likely worsen, and moisture will come down as unprecedented rainfall – or snow, if the local air mass is below freezing. Paradoxically, the above normal temperatures will also cause droughts and wildfires outside of historical patterns.

Preparing for this new era of extreme rainfall will be a huge challenge. Despite differences in preparing for the flooding from storms, extreme tides, rainfall, runoff, and rising sea level, the similarities may help when confronting the “water challenge” in a bold and thorough manner. People, cities, infrastructure, economies, and nations must adapt rapidly to environmental changes. Full recovery for the places affected by these three recent storms will take years. However, perhaps the “1-2-3 punch” of Harvey, Irma, and Maria will be a turning point for discussions and action to deal with the increased flooding in this new era. Those involved with emergency preparedness are on the front lines of flooding response and prevention.

John Englander is an oceanographer, consultant, and leading expert on sea level rise and related flooding. His broad marine science background with degrees in geology and economics, and personal experience in Greenland and Antarctica allow him to see the big picture on sea level rise and explain the phenomena in



CBRNE-TERRORISM NEWSLETTER – October 2017

plain language. Englander works with businesses and government agencies to understand the risks of sea level rise and the need for “intelligent adaptation.” He goes beyond the usual projections and explains the “uncertainties” that could yield considerably higher sea level as early as mid-century. His bestselling book, “High Tide on Main Street: Rising Sea Level and the Coming Coastal Crisis,” clearly explains the science of sea level rise, the impending devastating economic impacts and the opportunity to design for a more resilient future. He is a sought after speaker, having presented to national security leadership, the American Planning Association, American Institute of Architects, the U.S. Naval Academy, etc. He does a weekly blog and news digest “Sea Level Rise Now.”



ICI
International
CBRNE
INSTITUTE



ASYMMETRIC THREATS



'Syrian Lessons' and Russia's 'Asymmetric Response' to the US

Eurasia Daily Monitor Volume: 14 Issue: 118

By Sergey Sukhankin

Source: <https://jamestown.org/program/syrian-lessons-and-russias-asymmetric-response-to-the-us/>

Russian Krasukha-4 jamming complex (Source: Sputnik News)

Sept 26 – The Russian military operation in Syria has highlighted “urban warfare,” information security and **electronic warfare (EW)** as crucial elements of how Moscow envisions the “wars of the future” will be fought. **However, Russia's top brass is currently allocating a central role to the development of EW capabilities. Increasingly viewed by Russian military strategists as a pivotal tool for gaining and maintaining information superiority over its adversaries in future conflicts.** Russia's growing emphasis on the development of EW is inseparable from two events that occurred soon after Russia went into Syria. First was the November 2015 downing of a Russian Su-24 bomber by Turkish jets after it had strayed into Turkey's airspace. The second incident, reported on later that same month, involved Turkey deploying Koral electronic warfare complexes on its southern border in order to “dazzle” (blind) Russian S-400 air-defense missile systems that Moscow had just brought into Syria ([TASS](#), December 1, 2015). Incidentally, speaking from a historical prospective, Syria first became a training ground for the Soviet Army to test its EW capabilities as far back as 1982, following the outbreak of hostilities in Lebanon. And Moscow renewed those efforts in October 2015, when it deployed the Krasukha-4 multifunctional jamming station to the Hmeymin airbase ([Obzor.press](#), October 22, 2015), thus signaling a qualitatively new stage of Russian engagement in the Syrian civil war.

Analysis of Russia's performance in Syria when it comes to electronic warfare poses a number of challenges, of which the most important is the lack of uniformity in assessments produced by top Russian military experts. Some Russian sources clearly overestimate Russia's EW capabilities, asserting their total superiority over foreign analogues. Whereas others argue that “the lack of precision-guided munitions at the terrorists' disposal have made Russian systems such as the ‘Krasukha’ and ‘Khibiny’ almost irrelevant” on the Syrian battlefield ([Tvzvezda.ru](#), August 8).

Still, empirical evidence suggests that events in Syria (and of course in Ukraine—see [EDM](#), May 24) have spurred the Russian side to increase both its theoretical and practical efforts in upgrading EW capabilities. The most recent trends in this domain include:

- ◆ Import substitution and modernization: This past summer, the first deputy director of Concern Radio-Electronic Technologies (KRET), Vladimir Zverev, declared that “Russia has been able to fully substitute Ukrainian components in domestically produced EW technologies” ([Tvzvezda.ru](#), July 18). This development signifies that Russia has finally overcome its pre-2013 dependency on Ukraine in this sector. Moreover, KRET has reportedly begun work on a new land-based EW system designed to “replace” the Krasukha-2 and Krasukha-4 (photo) jamming stations ([Tvzvezda.ru](#), July 21), which might have a revolutionary effect on Russia's EW industry as such. Moreover, some sources have revealed that Russia has finalized work on a radio-photonic radar for a future sixth-generation fighter jet that will one day replace the Su-57 (T-50). The invention is said to be superior to “all existing radars when it comes to its power and range” ([TASS](#), July 27). According to a top-ranking KRET functionary, Vladimir Mikheev, the new device “will burn out the eyes of the missiles looking at us.”
- ◆ Spoofing, jamming and deceiving: Allegedly, KRET has created a new reconnaissance complex that can function even under “extremely difficult radio-electronic conditions” ([Tvzvezda.ru](#), July 18). Another potential invention—the Tarantul aircraft electronic countermeasures complex (ECM), which has been undergoing testing since 2007—will be integrated onboard the Su-34 fighter-bomber. One such system, when integrated into a single Su-34, is said to be capable of protecting a group of aircraft from enemy radar; and it has been described as “the future of Russian EW” ([RIA Novosti](#), August 28).
- ◆ New type of radio connection: On August 25, the head of the Armed Forces Communication Chief Department and the deputy head of the General Staff, Lieutenant-General Khalil Arslanov, stated that the Russian Armed Forces tested in Syria a new type of “secure communications.” This system could effectively replace previous models (used by the Syrian Army) that were discredited in the course of the Palmyra, Deir ez-Zor and Idlib operations ([Rosbalt](#), August 25). The main idea behind Russia's new invention is based on the use of so-called “trunked



CBRNE-TERRORISM NEWSLETTER – October 2017

systems” (radial-zonal systems) of communication, capable of an automatic distribution of channels among different user groups.

Russia’s conceptual approach to the development of EW capabilities was recently outlined by the editor-in-chief of *Arsenal Otechestva*, Victor Murakhvoskii, who specifically defined it as an “asymmetric response” ([Pravdinform](#), August 28). The expert argued that Russia (due to its economic hardships and the smaller size of its domestic economy) is unable to directly engage the United States in competition in



all areas and domains. Instead, he suggested, Russia needs to achieve “technological superiority in key branches of the domestic Armed Forces.” Given Russian perceptions of how the “wars of the future” will be fought, Murakhvoskii identified air, naval and EW capabilities as prime capabilities in which Russia has to develop its superiority.

On the other hand, it might well be expected that in light of the experience gained in Ukraine and Syria, Russia will also attempt to focus on “cyber warfare” (primarily cyber operations) and “electronic warfare.” Such an emphasis would become apparent if the Russian Armed Forces are repeatedly observed carrying out military exercises whereby they practice corrupting or disabling a simulated adversary’s Command, Control, Communications, Computers, Intelligence, Surveillance and Reconnaissance (C4ISR) systems. In the final analysis, when assessing the key trends and developments in Russia’s EW capabilities being honed in Syria, one needs to keep in mind that aside from being an actual battlefield, Syria has also become a theater of violent information warfare (primarily information-psychological operations). In such an environment, truth and disinformation are not easily distinguishable. Thus, Russian claims regarding EW should be treated with a healthy dose of skepticism.

Sergey Sukhankin is a historian from Kaliningrad and Associate Expert at the International Centre for Policy Studies (Kyiv). His area of scientific interest primarily concerns Kaliningrad and the Baltic Sea region.





BUSINESS CONTINUITY

OPEN FOR
BUSINESS
AS USUAL

Business Interruption

Disaster Event

Is Your Company Ready to Face Tomorrow's Security Risks?

By Maciej Rosolek, Paulina Świątek and Malgorzata Zabieglinska-Lupa

Source: <https://www.infosecurity-magazine.com/blogs/is-your-company-ready-tomorrows/>

Oct 09 – In 2017, ransomware, phishing, and IoT attacks pummeled businesses. What security trends will emerge in the coming years? Malgorzata Zabieglinska-Lupa, ICT product manager, [Comarch ICT](#), recently had the chance to speak to Paulina Swiatek, business solution manager, and Maciej Rosolek, IT risk & security department manager, about trends in the security technology market and what companies can do to protect themselves.

Malgorzata Zabieglinska-Lupa: Security is one of the fastest growing sectors in the IT market. The hot areas for security growth are security analytics, SIEM tools, threat intelligence, mobile and cloud security. Why is security always a catch-up game?

Maciej Rosolek: I'll try to answer this question as illustratively as possible. Protective measures taken by security departments throughout the world can be compared to a dam on a river, with the river standing for malicious people's activities. We build a dam to resist pressure from the river – applying best practices, available knowledge and experience.

Now having a dam, we feel safe, protected against a potential flood. After some time, the water will erode our dam. When the breaches are tiny, we can easily fix them, but as time passes there are more and more leaks, as water doesn't give up easily and finds new cracks to go through. The situation arises in which it is impossible or uneconomical to fix our dam further. On the basis of the experience gained during fixing the first dam, we build another one which is stronger, tighter, and therefore safer. However, the river is relentless, it becomes more and more rapid, and after some time our dam starts to leak again. This is more or less how our work looks (by 'our' I mean security teams around the world).

According to best practices, knowledge and experience, we develop protection which is then penetrated by people who want to get to the other side. As a result of the development technological advances and high computing power accessible to everyone, there are more and more tools which make it possible for hackers and crackers (malicious people) to drill tunnels in our dam, which must be fixed immediately.

Paulina Swiatek: The world of IT is rapidly changing; the quickest changes can be seen in the development of intrusions and attack methods. Sometimes it seems that hackers are the fastest learning IT sub-group. Hence, security could be seen as a catch-up game. To anticipate an attack, we must be a step ahead of the hackers. Of course, it is difficult to achieve this without the appropriate expenditure on employee training and investment in IT infrastructure. This is why it might be said that, in this game, the success of a hacking attack may be related directly to the time and money that will be spent on this purpose.

Malgorzata Zabieglinska-Lupa: Have you seen any major change in organizations' attitudes to security in the past few years? Is it a strategic business consideration, or is it still considered something separate?

Paulina Swiatek: Security has always been seen as a cost, and therefore the question arises... is it really necessary? Hopefully, this perspective is changing, partly because hacking attacks, of different kinds, are more and more common. It is really hard to avoid hearing about them, for example when UK hospitals were hit with massive ransomware attacks, when sensitive documents possessed by Edward Snowden were leaked, or when intimate photographs of a celebrity make their way into the public eye. It's the kind of news that hits us every day and makes people think more seriously about IT security. There are also more and more companies that have been hacked, and now their owners understand that you can lose much more money when you are hacked than you might have spent on IT security solutions to protect against those attacks. IT security strategy should be considered and built together with business strategy. Unfortunately, this is not always the case. Treating a company's IT security and its strategy as separate issues makes IT security more expensive and less in line with a company's needs.

Malgorzata Zabieglinska-Lupa: What trends do you think we'll see in the IT security space in the next few months?

Maciej Rosolek: Each day brings new threats – at the last security conference I learned that more than 100,000 new viruses/malware elements were created daily. It is hard to cope with such an avalanche of threats using 'ordinary' anti-virus software based on signatures, or using people to analyze logs and security events. We need automatic 'thinking' solutions which will be



CBRNE-TERRORISM NEWSLETTER – October 2017

able to recognize, on the basis of the analysis conducted, whether a particular file or action can pose a threat.

Therefore, we are talking about all kinds of security devices with machine learning functionality, including:

- SIEM tools which have to correlate data from various sources, and, on that basis, decide whether a given system/user behavior indicates a potential intrusion
- IPS/IDS systems with learning functions
- Flow analysis systems with learning functions
- And many other 'intelligent' solutions...

I believe that machine learning will be the functionality that complements security systems and improves the security of organizations and of the data entrusted to them.

Paulina Swiatek: In relation to the new EU directive – GDPR – coming into force in May 2018 – it can be assumed that many companies will be forced to analyze, verify and improve the quality of their IT security. Otherwise, they may be exposed to significant financial penalties. A lot of companies do not have the required resources, especially when it comes to the competence of their IT security employees, so they will need support from external companies that specialize in IT security (IT integrators and IT service providers). All this should lead to a trend showing an increase in IT security spending.

Malgorzata Zabieglinska-Lupa: Paulina started to talk about GDPR. Can you elaborate on this topic? How will this regulation impact security strategies in companies? How can a company be ready for all the changes that GDPR will bring?

Maciej Rosolek: The EU Regulation on Personal Data Protection has been widely discussed recently, but frankly speaking, if it weren't for the horrendous penalties for disclosing personal data set out in this regulation no one would probably care about this issue. Why do I say that? The Act on the Protection of Personal Data was produced – correct me if I'm wrong – in 1997. It has been amended several times, but have its provisions been observed? I guess that aware companies and businesses have observed them, but they constitute only a small percentage of enterprises which store or process sensitive data. I will not conceal the fact that I'm pleased with the provisions of this Resolution – I hope that it will lead to many companies treating security issues with due diligence, protecting what is important for us – our personal data.

How should we prepare ourselves for changes? First and foremost, the Resolution has to be read and understood, places where personal data are stored have to be located, and it should be checked who has access to the data and how many 'paths' lead to them. Then, a risk analysis should be carried out and processes and 'proper protections' should be devised. When it comes to protection, there is no one 'template' such as 'You have to equip yourself with A, B, C or D systems/devices'. Everyone should find the appropriate solutions to protect data stored or entrusted to them.

Malgorzata Zabieglinska-Lupa: No matter how many security solutions are implemented, enterprises will always be a target for cyber-thieves. How can a successful IT security strategy be developed? What should companies focus on?

Paulina Swiatek: IT security strategy should take into account a few important factors, such as business and corporate strategy, IT strategy, compliance and standards, regularly repeated analysis of threats, risks and current security state. The starting point for building an IT security strategy should be the determination of goals and direction of the company and its business. Then, the assessment of the current security state should take place. Within this assessment, deep knowledge of the company, its processes, functions and business is needed. The security strategy should always be compatible with the business and company strategy, taking into account future plans and products. If we know where we are, and we understand where the company is heading, we can start working on specifying the desired state of the company's security and methods, including the steps and detailed phases required to get us there. It is worth remembering that IT security is constantly changing, which forces us to review our IT security strategy level constantly, and to measure its effectiveness and make improvement where required.

Malgorzata Zabieglinska-Lupa: To close, I would like to ask both of you how end users can be made aware of the importance of data security and privacy?

Paulina Swiatek: The end user is always the weakest point in the company's IT security. Even the most elaborate, professional tools, that cost a fortune, will not do anything unless employees are aware of the dangers and how they should behave. Today, making users more aware of security seems to be a bit easier, because we see more and more news about data leaks. Irrespective of this, we should initially assume that employees have a very low



CBRNE-TERRORISM NEWSLETTER – October 2017

level of IT security awareness. It is also good practice to carry out periodic employee security training, with mandatory exams to test knowledge of the company's security policy and how to handle and deal with sensitive information in order to avoid violating that policy and exposing yourself or the company to leaks of confidential data.

Maciej Rosolek: This question touches on a key security issue (and threat) for our sensitive data, and the end users constitute this threat. The security of the data stored in companies relies mainly on the knowledge and awareness of end users. It is therefore of utmost importance to carry out awareness-raising actions and information campaigns on basic security issues, such as:

- Password policy
- Giving access to data from the user's account to third parties
- Copying data to a local drive
- Susceptibility to socio-technical attacks
- And many more

All issues are described in the company's security policy. It also defines the necessity to carry out awareness-raising actions for employees. Each newly appointed member of staff should attend training on security issues and take a test afterwards. That is not all. In order to consolidate this knowledge, each employee should review security issues and take a test at least once a year. Additionally, there should be security events organized for employees, where methods for obtaining data are shown, and where employees are made aware of possible socio-technical attacks. There are plenty of ways...current technology gives us many tools for communication – we just have to be willing to use them.

Maciej Rosolek is IT Risk & Security Department Manager, Comarch ICT.

Paulina Świątek is Business Solution Manager, Comarch ICT.

Malgorzata Zabieglinska-Lupa is ICT Product Manager, Comarch ICT.

