

Dedicated to Global First Responders

CBRNE

NEWSLETTERRORISM



November 2017



www.cbne-terrorism-newsletter.com

IOI
International
CBRNE
INSTITUTE



DIRTY R-NEWS

Nuclear terrorism: Before it's too late

By Yonah Alexander and Milton Hoenig

Source: <https://www.timesofisrael.com/nuclear-terrorism-before-its-too-late/>

Oct 25 – Does President Donald Trump's [recent declaration](#) that he will not certify Iran's compliance with the 2015 Joint Comprehensive Plan of Action increase the likelihood of a potential unconventional war in the Middle East or contribute to international efforts to prevent nuclear terrorism? Make no mistake. While the debate over the answer to this key question will continue in the coming months and years, nuclear terrorism, considered by both state sponsors and sub-state entities, will remain a clear danger to regional and global security concerns and perhaps even to the survival of civilization itself.

More specifically, the Iranian threat has indeed increased in scope and intensity with every passing year. In the 1990s, Tehran acquired some nuclear capabilities and subsequently contracted with Russia to build a nuclear power reactor that began operation in 2011, in addition to its small research reactor acquired from the United States in 1967. A decade later, Iran had succeeded in developing a robust nuclear infrastructure for uranium ore processing and uranium centrifuge enrichment. Additionally, it has undertaken programs of dual-use chemical and biological technologies as well as advanced missile defensive and offensive weapons. And, as recently as August 2017, Tehran warned that in the event the US imposes new sanctions, it would need only five days to ramp up uranium production to 20 percent, up from the enrichment level of below 3.67 percent under the current deal. This would potentially amount to some 90 percent of the enrichment work for uranium needed to build a nuclear bomb. In the interim, Iran has rejected US demands for UN inspectors to examine military sites in the country.

Other recent and relevant stark security concerns include testing successfully the Khorramshahr ballistic missile capable of carrying nuclear warheads more than 1,200 miles; launching new satellite missiles; building precision weapons factories in Syria and Lebanon; advancing and deploying cyber-spying prowess regionally and over Western airspace; and continuing to finance and supply weapons to terrorist groups in the Middle East and to Africa's expanding arc of instability.

The potential challenge of global terrorist groups obtaining weapons of mass destruction cannot be dismissed.

Within the context of these worrying developments, the most troubling emerging challenge to global security is Iran's proxy Hezbollah ("Party of God"), the most dangerous terrorist movement in modern times. In this regard, the August 13, 2017 warning by Hassan Nasrallah, Secretary General of Hezbollah, alarmingly hints at a planned attack on Israel's Dimona nuclear facility in an effort to release radioactivity into the environment. In a televised address he boasted, "One example of the respect and recognition Israel gives the 'resistance' is the closure of the ammonia tank in Haifa...We hope that they will look into moving the nuclear reactor in Dimona as it is more dangerous and needs extra care."

This ominous threat to Israel is also a reminder that Hezbollah even has the potential to undertake terrorist attacks directed against America itself. Thus, Nicholas Rasmussen, the director of the US National Counterterrorism Center (NCTC), stated on October 11, 2017, that "we in the intelligence community do in fact see continued activity of Hezbollah here inside the Homeland." It is no surprise that the US Department of State has just announced rewards for information about two senior operatives of Hezbollah who helped the suicide attack on the US Marine command in Beirut in October 1983, killing 251 servicemen: \$7 million for information about Talal Hamiyah and a \$5 million bounty on Fu'ad Shukr.

The potential challenge of global terrorist groups obtaining weapons of mass destruction cannot be dismissed. For example, al-Qaeda has already demonstrated its interest in acquiring weapons of mass destruction over the past two decades. As early as 1998, Osama bin Laden stated that acquiring WMD is a "religious duty." Ample evidence was discovered that al-Qaeda training camps in Afghanistan focused attention on utilizing biological, chemical, radiological, and "dirty bomb" capabilities if available. Also, earlier in Sudan, a bin Laden associate had tried to buy uranium for a nuclear weapon.



CBRNE-TERRORISM NEWSLETTER – November 2017

More recently, Daesh (also known as the Islamic State, ISIS, or ISIL) is believed to be responsible for a 2015 mustard gas attack in Syria and reportedly intends to pursue other WMD capabilities. Just imagine what might have happened if Raqqa, the declared capital of the “Islamic Caliphate”, had not been liberated, or more territory had been ceded elsewhere to Daesh. The surviving leadership and its die-hard members might yet resort to WMD attacks in their battle for regional and global dominance. The most challenging danger of nuclear terrorism comes into play if states or sub-state groups succeed in achieving their strategic goals. The temptation for other actors to resort to nuclear or other WMD capabilities may become inevitable. Can we prevent this tragic eventuality? The short answer is yes, but only if we remain steadfast in our determination to do so.

It therefore behooves the international community to urgently expand their current counterterrorism and non-proliferation efforts. These include terminating all business relationships between western companies and Iran’s Revolutionary Guard so long they continue to destabilize the Middle East through violence. Greater control of illicit trafficking of WMD materials should also be instituted regionally and globally, coupled with contingency planning and crisis management policies to reduce nuclear terrorism risks.

The cost of escalation to war, even with the high likelihood that the West would prevail, would be terrible beyond measure. All nations, including Iran and North Korea, would be wise to heed the Persian proverb, “Even with the strength of an elephant and the paw of a lion, peace is better than war.”

Yonah Alexander is a professor emeritus at the State University of New York, the director of the Inter-University Center for Terrorism Studies, and Senior Fellow at Potomac Institute for Policy Studies.

Dr. Milton Hoenig is a nuclear physicist based in the Washington, DC area.

identiFINDER R440

Source: http://www.flir.com/threatdetection/r440/?utm_source=launch&utm_medium=email&utm_campaign=r440&utm_content=banner

The FLIR identiFINDER R440 is a lightweight, sourceless radioisotope identification device (RIID) that can be operated with one hand and is IP67-rated to survive tough missions. Not only does the 2x2 NaI detector deliver sensitive and fast detection, but it also provides accurate identification during secondary screening. The new 360° EasyFinder™ Mode expedites decision-making to keep you safe.

2x2 NaI detector

3.5x more sensitive than other general all-purpose RIIDs and provides up to 10% better resolution; extended energy range provides neutron indication.

Sourceless stabilization

Automated stabilization improves data collection and reduces false positives to expedite decision-making in the field.

IP67-rated

Protected from total dust ingress and water immersion up to 1 meter in depth for up to 30 minutes (rain, splashing and accidental submersion).

Rugged construction

Drop-tested to 1 meter and built to survive rigorous missions, with completely enclosed crystal. Fully meets the ANSI N42.34 standard.



CBRNE-TERRORISM NEWSLETTER – November 2017**360° easyfinder mode**

Collects and interprets data, then pinpoints the exact location of source for user so they can easily navigate and respond to threats.

Wireless communications

Built-in feature enhances interagency standardization and improves response options. Standardized file format meets ANSI N42.42 standard.

Specifications

Model Number	FLIR R440
Technology	Radioisotope identification device (RIID)
Gamma - NaI(Tl)	2.0 x 2.0 in (51 x 51 mm)
Gamma / Neutron - NaIL (optional)	2.0 x 2.0 in (51 x 51 mm)
Energy Range (Gamma)	10 keV to 10 MeV
Gamma Sensitivity (Cs-137, NaI)	1850 cps/μSv/h
Gamma Spectrum Length	1024 channels
Dose Rate Range (Cs-137, NaI)	10nSv/h - 10mSv/h (1μrem/h - 1rem/h) / ±30 %
Dose Rate Range ID Mode (Cs-137, NaI)	10nSv/h - 250μSv/h (1μrem/h - 25mrem/h)
Overload Dose Rate Range (Cs-137, NaI)	10mSv/h - 500mSv/h (1rem/h - 50rem/h)
Stabilization	Sourceless gain stabilization (patents pending)
Linearization	Real-time linearization of gamma energy
Typical Resolution	≤7% FWHM at 662 keV with NaI detector at 20 °C
Service Interval	1 year factory maintenance suggested, not required

Sampling & Analysis

Sample Introduction	Absorption of EM gamma (NaI) or gamma and neutron emissions (NaIL)
Threats	Detects neutron or gamma radiation emitted from natural occurrences in the environment, special nuclear material, industrial, or medical material
Nuclide Identification	According to ANSI N42.34
Library Categories	SNM, IND, MED, NORM
Time to Alarm	From a few seconds to minutes

System Interface

Display & Alerts	Transflective color LCD / 3" (2.72" x 1.61") Color TFT Display, Resolution: 800 x 480 pixels
Communication	USB 2.0, USB OTG; Bluetooth® Class 2.0 ≤10m range (removable); WiFi 802.11 g/n
Data Storage	32GB internal memory
Training Requirements	<10 mins for operator; 1 day for advanced user
GPS (removable)	12-channel SiRF III receiver



CBRNE-TERRORISM NEWSLETTER – November 2017

Software	On-board webserver software
Power	
Input Voltage	100-240V AC (wall adapter and USB cable supplied)
Battery Specs	Supplied: 2x rechargeable Li-Ion smartpacks and 1x 4x AA pack; ≤6h runtime with one Li-Ion smartpack, ≤12h with both Li-Ion; runtime of ≤4h with AA battery pack (Li-Ion); Optional rechargeable NiMH ion smartpack with ≤5h runtime; recharge ≤4h when using AC; recharge >4h when using USB; run times specified are obtained with a mix of Dose Rate, Finder, and ID operating mode
Cold Start Time	<2 mins from cold start
Environmental	
Operating Temp (ambient)	-4 to 122 °F (-20 to 50 °C)
Operating Humidity	10 to 80%
Storage Temp	14 to 95 °F (-10 to 35 °C)
Physical Features	
Dimensions (L × W × H)	≤ 4 x 10.6 x 3.7in (10.2 x 26.9 x 9.4)cm - with battery
Weight	≤3.2 lbs (≤1.5 kg)
Enclosure & Protection	Aluminum housing; protection rating IP67 according to IEC 60529

Korea War Seen Killing Up to 300,000 Even Without Nukes

By Anthony Capaccio

Source: <https://www.bloomberg.com/news/articles/2017-10-27/new-korean-conflict-could-kill-300-000-within-days-report-says>

Oct 27 – Renewed conflict on the Korean peninsula could kill hundreds of thousands of people in the first few days alone even if no nuclear weapons are involved, according to a new report by the Congressional Research Service.

Given population densities on the peninsula, military conflict “could affect upwards of 25 million people on either side of the border, including at least 100,000 U.S. citizens,” according to a 62-page assessment sent to U.S. lawmakers Friday and obtained by Bloomberg News.

The grim report comes after tensions between the U.S. and North Korea peaked over accelerated missile and nuclear weapons tests by Kim Jong Un’s regime, exacerbated by a war of words between Kim and President [Donald Trump](#). Earlier Friday, Defense Secretary Jim Mattis visited the demilitarized zone between North and South Korea, saying the U.S. is continuing to pursuing diplomacy as the preferred choice to resolve the crisis.

Yet with the U.S. also saying that all military options are on the table, the CRS report laid out in sharp detail the consequences of a conflict. North Korea can rely on hundreds of thousands

of artillery rounds within striking distance of Seoul, making it difficult for even a preemptive strike to prevent mass casualties.

Even if North Korea “uses only its conventional munitions, estimates range from between 30,000 and 300,000 dead in the first days of fighting,” the report said, citing North Korea’s ability to fire 10,000 rounds per minute. Moreover, the conflict could quickly spread to involve forces from China, Japan and Russia.

“Such a conflict could also involve a massive mobilization of U.S. forces onto the Korean Peninsula, and high military casualty rates,” the report said. “Complicating matters, should China choose to join the conflict, those casualty rates could grow further, and could potentially lead to military conflict beyond the peninsula.”

Still, the report noted that some analysts say that allowing Kim’s regime to acquire the ability to develop a missile capable of delivering nuclear warheads to the continental U.S. would be of even greater risk than the outbreak of regional war.

Trump is scheduled to visit South Korea as part of a tour through several Asian nations starting next



CBRNE-TERRORISM NEWSLETTER – November 2017

week. U.S. Secretary of Defense James Mattis, in Seoul for annual military talks, reiterated Saturday that the use of any nuclear weapons by North Korea would be met with a “massive” response and said the threat had accelerated from earlier this year.

Bannon’s Warning

Former senior Trump adviser Steve Bannon underscored the dangers of U.S. military strikes in August when he said in an interview with *The American Prospect* that “until somebody solves the part of the equation that shows me that ten million people in Seoul don’t die in the first 30 minutes from conventional weapons, I don’t know what you’re talking about, there’s no military solution here, they got us.”

CRS doesn’t go as far as Bannon, but its assessment presents lawmakers with a sobering view of what conflict could look like if the U.S. takes preemptive action against North Korea with the “fire and fury” Trump has threatened to rain on Kim.

“Few analysts believe that North Korea would launch an unprovoked attack on U.S. territory” but as the crisis continues to evolve “Congress could confront significant questions regarding its role in shaping U.S. policy in the region,” it said. At the same time, U.S. sanctions, diplomacy, and military shows of force “have arguably slowed” but “not halted the advance of North Korea’s” weapons of mass destruction programs, CRS said.

The assessment acknowledges the pressure facing the Trump administration is heightened by the view of intelligence and military advisers that by next year North Korea is likely to have mastered all of the technology for an intercontinental ballistic missile capable of hitting the U.S.

Urgency of Talks

“This assessment implies that the timeframe for conducting military action without the risk of a North Korean nuclear attack against U.S. territory is narrowing” and “may increase the urgency of efforts to restart multilateral

diplomatic efforts,” it said. Some analysts maintain that the road to negotiations “could be strengthened and accelerated if both North Korea and China believe that a U.S. military strike” is “becoming more likely,” CRS said.

White House Chief of Staff John Kelly said as much at an Oct. 12 press conference. Citing North Korea’s ICBM threat, he said, “Right now, we think the threat is manageable, but over time it -- if it grows beyond where it is today -- well, let’s -- let’s hope diplomacy works.”

Secretary of State Rex Tillerson said this month that diplomatic effort will continue “until the first bomb drops.”

The CRS report also explored the possibility that a war between the U.S. and North Korea would quickly turn into a wider conflagration.

“A protracted conflict -- particularly one in which North Korea uses its nuclear, biological, or chemical weapons -- could cause enormous casualties on a greater scale, and might expand to include Japan and U.S. territories in the region,” said CRS. “Such a conflict could also involve a massive mobilization of U.S. forces onto the Korean Peninsula, and high military casualty rates.”

Clash With China

The U.S. also “runs the risk of a direct military clash with China,” as occurred during the Korean War of 1950-1953, CRS said. It called China’s reaction “perhaps the most significant geopolitical question arising from a military conflict.”

Preemptive U.S. strikes “could risk a major rupture in its relationship with China,” which is the top U.S. trading partner and holds as much as \$1.15 trillion in U.S. bonds as of June, CRS said. The Trump administration has pressed China to cut off trade and exert other pressure North Korea to stop its nuclear program.

In addition to the horrific human toll of dead and wounded war on the Korean Peninsula, CRS said, a war “could lead to massive flow of refugees into northeastern China, where large numbers of ethnic Koreans reside.”

The persistence of the radioactive bogeyman

By Andrew Newman

Source: <https://thebulletin.org/persistence-radioactive-bogeyman11212>

As the gigantic ants—mutations born of the first nuclear weapon test in New Mexico—are exterminated by US army flame-throwers in the climactic scene of 1954’s *Them!*, Dr. Harold Medford reflects: “When man entered the atomic age, he opened the door to a new world.



CBRNE-TERRORISM NEWSLETTER – November 2017

What we'll eventually find in that new world, nobody can predict." In the world of horror cinema, however, the results are entirely predictable. Bad and scary things come of meddling with the atom.

Most movie buffs know about Godzilla and Mothra, but the range of radiation-themed horror movies extends far beyond those Japanese monsters. Since 1950, in fact, a remarkable number of American and European horror movies have used radiation as a central plot device. It is a rich, if not distinguished, history. In fact, it is a mostly miserable history, full of bad production values, bad plots, and bad acting. But that doesn't mean these radioactive B-movies are unimportant. They reflect the fears and misconceptions of their era as they relate to scientific advances—and scientific arrogance.

Horror, science, and radiation

At the beginning of the 20th century, "excited physicists pointed out that for countless ages radium has been emitting heat and light while transmuting, as though it contained the energies of the original creation. When doctors reported that atomic rays could heal they seemed only to confirm that radioactivity meant life-force." Indeed, as Spencer Weart's book *Nuclear Fear* notes, in 1903 a Connecticut newspaper suggested that radium could plausibly raise the dead. Reflecting on his radium-based miniaturization experiments in *Dr. Cyclops* (1940), Dr. Thorkel declares: "In our very hands we have the cosmic force of creation itself ... we can shape life, take it apart, put it together again, mold it like putty." His colleague, Dr. Mendoza, objects: "But what you are doing is mad. It is diabolic. You are tampering with powers reserved to God." Thorkel, clearly thrilled by the suggestion, responds: "That is good. That is very good. That is just what I am doing."

But by 1945, radiation had acquired an even more insidious reputation in the real world. The awful fates of [Marie Curie](#), the "[Radium Girls](#)" who died from painting luminous radium paint onto dial faces, steel company president [Eben Byers](#), who died from drinking Radithor, a radium-laced tonic, and the residents of Hiroshima demonstrated the ghastly destruction that this odorless, flavorless, invisible force could wreak on the human body. It did not require a huge leap of faith for moviegoers to imagine that ionizing radiation could also cause miniaturization, gigantism, and terrible mutation.

Horror movies' primary purpose is to scare the audience, and as a rule, the genre is quite conservative, reinforcing society's rules and punishing transgressors. Given a deep public ambivalence toward scientific discovery, scientists have been big losers in horror films. In 1950s and 1960s cinema, science experiments were rarely portrayed as nefarious by design. All the same, they were held responsible for some horrific threat manifest in the world—but it was a threat that scientists also had the expertise to combat, usually by destroying the monster (with the help of the military). But by the 1970s, corporate/government/ military conspiracies are the norm; scientists unleash forces they cannot control, and the end of the movie is far from the end of the story.

The atomic monster cycle

The successful 1952 re-release of *King Kong* (1933) encouraged Warner Brothers to launch the atomic monster cycle film, film critic Kim Newman writes in his book *Apocalypse Movies*. And audiences loved it. By the mid-1950s, "if it wasn't atomic and didn't glow in the dark, it wasn't going to sell," Jamie Russell notes in *Book of the Dead: The Complete History of Zombie Cinema*. With the exception of *The Incredible Shrinking Man* (1957), bigger

and angrier was the sure-fire result of irradiation by good, bad, or indifferent scientists.



Scene from *The Beast From 20,000 Fathoms*. Photo credit: [Wikimedia Commons](#)

In *The Beast From 20,000 Fathoms* (1953), US nuclear weapons tests in the Arctic wake a 100 million year old "rhedosaurus." The



CBRNE-TERRORISM NEWSLETTER – November 2017

creature is shot with and killed by a radioactive isotope, providing one of the clearest illustrations of the thin line between nuclear science destroying the world and saving it.

In *Them!*, Warner's highest grossing movie of 1954, giant ants leave a trail of death and destruction in New Mexico and, briefly, Los Angeles. However, in what is as close as 1950s horror came to an open ending, Dr. Medford muses: "We haven't seen the end of them. We've only had a close view of the beginning of what may be the end of us"—a fair point to make, given that the United States didn't conduct its last atmospheric nuclear test until July 1962, with underground tests continuing till September 1992.

In *It Came From Beneath The Sea* (1955), a giant octopus causes havoc on the San Francisco waterfront before being blown to bits, hydrogen bomb tests in the Marshall Islands having irradiated the cephalopod and scared off all of the other sea creatures, forcing it to the surface in search of food.



In *X the Unknown* (1956), a subterranean explosion in the Scottish Highlands releases a blob-like ooze that destroys property and gives several non-essential cast members radiation burns.

Conveniently, experiments with fictional radioactive element "trinium" are successful just in time to

neutralize the life form. The subversive ramifications are clear: It is now possible to "neutralize" atomic bombs. (A Cold War side note: Film buffs may recall that Joseph Losey, who had fled to London several years earlier when brought to the attention of the House Un-American Activities Committee, directed *X* for a few days before "falling ill." Star Dean Jagger's refusal to work with a communist sympathizer had in fact forced Hammer Films to replace Losey.)

In Roger Corman's *Attack of the Crab Monsters* (1957), nuclear testing in the Pacific creates a couple of massive crabs. Any matter they eat is assimilated, enabling the crustaceans to make use of human faculties, such as holding conversations with surviving cast members, who eventually electrocute the last of the monsters.

In *Beginning of the End* (1957), the Department of Agriculture under the direction of a pre-*Mission Impossible* Peter Graves is using radioisotopes to grow enormous vegetables. But the produce attracts hungry locusts, which then mutate to gigantic size before drowning in Lake Michigan. Director Bert Gordon liked the concept so much he also helmed *The Cyclops* (1957), *The Amazing Colossal Man* (1957) and *War of the Colossal Beast* (1958), all of which also deal with the power of radiation.

In *Fiend Without A Face* (1958), a professor diverting power from a nuclear reactor for thought-materialization experiments inadvertently creates "mental vampires" that attach themselves to hapless victims. Eventually realizing the error of his ways, the scientist sacrifices himself helping the military blow the reactor up.

In *The Alligator People* (1959), a doctor treats accident victims with an alligator protein in the Louisiana bayou. However, the patients begin to exhibit gator features. A radical procedure to treat these gator-humans—[cobalt 60](#) gamma rays and x-rays—is sabotaged, and the first test subject transforms into an alligator man before he sinks into a swamp.



CBRNE-TERRORISM NEWSLETTER – November 2017

In *The Hideous Sun Demon* (1959), a doctor is irradiated while working with a new isotope. As a consequence, sunlight causes him to devolve into a scaly prehistoric creature. As the transformations increase, so do the creature's homicidal urges, but even when bludgeoning policemen, the creature has the decorum to wear dress pants before being shot.

In *Atom Age Vampire* (1960), a professor must harvest cells from young women to replenish a serum that treats accident victims. Lacking the intestinal fortitude to carry out this task, he uses another serum to transform into a homicidal monster and then irradiates himself back to normal. When the transformation to monster becomes permanent, the scientist is killed by his mute assistant.



In *The Beast of Yucca Flats* (1961), a defecting Russian scientist is transformed into a crazed killer by a nuclear test before being shot.

And in *Die, Monster, Die!* (1965), Boris Karloff reprises his 1936 role in *The Invisible Ray*: a scientist whose experiments with meteor radiation are rooted in benevolence but end in death and self-destruction.

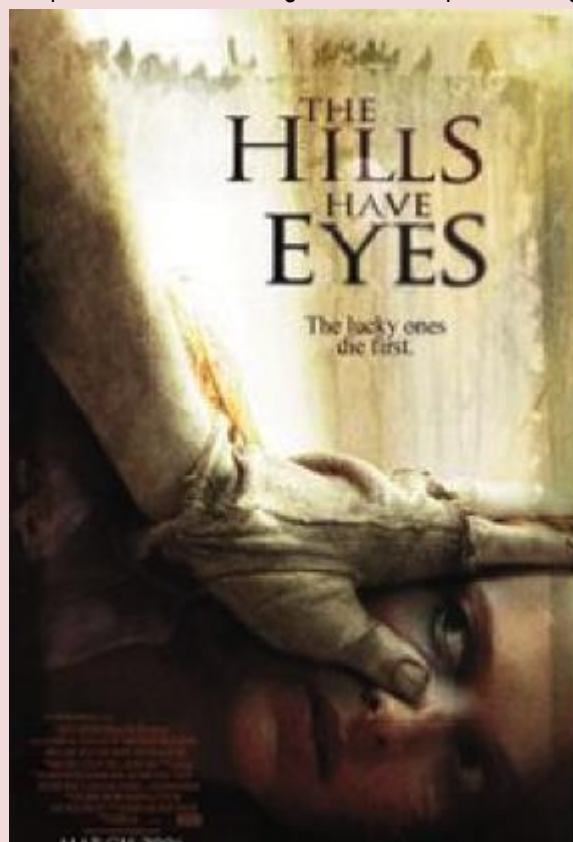
The modern era

Alfred Hitchcock's *Psycho* (1960) introduced audiences to the future of horror. However, not until 1968 would the

radioactive bogeyman shamble, in black-and-white, into the modern era ... in Pittsburgh. In George Romero's landmark *Night of the Living Dead*, causation is never proven, but speculation centers on radiation from a destroyed satellite that is reactivating the brains of the dead. Thus: kill the brain, kill the ghoul. In *Let Sleeping Corpses Lie* (1974), images of pollution, overcrowding, and nuclear plant cooling towers grace the beginning of the film. "Ultrasonic radiation" is being used to destroy insects, but it also brings back the dead. Set in England and filmed in color, the movie draws from Romero yet achieves a creepiness all of its own.

In *The Being* (1983), the fictional Pottsville, Idaho is host to a waste disposal facility and a series of unexplained murders. A haughty scientist and government flack concludes that a young boy with damaged chromosomes was irradiated at the site, creating a creature that uses a higher percentage of its brain and is completely psychotic! In *C.H.U.D.* (1984), the homeless living underground are disappearing because radioactive and other waste is being dumped in the New York City sewers; the government's Contamination Hazard Urban Disposal (C.H.U.D.) program is turning the vagrants into Cannibalistic Humanoid Underground Dwellers (C.H.U.D.s). Umberto Lenzi's otherwise abysmal *Nightmare City* (1980) is notable in this context because the marauding mob is the product of a radioactive spill at a power plant.

In 2006, Alexandre Aja re-made, and slightly reinterpreted, Wes Craven's 1977 tale of inter-familial savagery *The Hills Have Eyes*. The movie opens with a written admonition: "Between 1945 and 1962 the United States



CBRNE-TERRORISM NEWSLETTER – November 2017

conducted 331 atmospheric nuclear tests. Today, the government still denies the genetic effects caused by the radioactive fallout ...” Why the filmmakers chose 331 is unclear; 210 is the correct number. In Aja’s vision, before the US nuclear weapons testing program could begin, local residents were relocated. Some hid in the mines and it is their offspring that begin murdering a family on a cross-country trip. A grosser sequel was released in 2007.

Meanwhile, the military was busy creating its own exotic weapons systems. In *Piranha* (1978), genetically modified and irradiated fish bred for use in Vietnam are unwittingly released upstream of a Texas community enjoying a summer day in the river; carnage ensues. A sequel of sorts, *Piranha II: The Spawning* (1981), was directed by debutant James Cameron but there is little evidence of the talent that would helm *The Terminator* three years later. In *It’s Alive III: Island of the Alive* (1987), the murderous mutant children of the first two movies are relocated to an island used for secret nuclear tests. A team of scientists predict a Darwinian up-side: “We see them as a jump in the evolutionary pattern; creatures capable of surviving a nuclear holocaust, withstanding radiation, even thriving on it.” In *Spontaneous Combustion* (1990), a shadowy corporation uses an anti-radiation drug to create a man with the ability to ignite people and be “the world’s most sophisticated nuclear weapon.”

There have also been several radioactive zombie comedies (*Fido*, 2006; *Dance of the Dead*, 2008) and some more (*Mansquito*, 2004) or less (*Teeth*, 2008) conventional creature features.

A decaying bogeyman?

In November 1945, Assistant Secretary of War John McCloy reported the “locust-like effects” of the Red Army, a threat that manifested quite literally in *Beginning of the End*. As Peter Biskind notes in his 1983 book *Seeing is Believing*, the incredible mutations of the early Cold War movies most obviously represented communism: primitive aggressive hordes or emotionless repressive automatons depending on your political philosophy. Either way, in little more than an hour the monster was destroyed and normality restored; a victory for “us” over “them.”

With Romero and Roman Polanski’s infamous final Satan’s-child scene in *Rosemary’s Baby* setting the stage in 1968, modern era horror embraced the post-Vietnam/Watergate aesthetic, as the locus of the horror shifted from them to us. While plots are still largely driven by experiments gone awry, authorities are the conspirators, innocent people become the monsters, and nuclear power is just as dangerous as nuclear weapons—a conviction confirmed for some by the Three Mile Island accident in 1979. Creature features survive, but they are an increasingly small minority, and in a subtle but important change, the monsters are engineered rather than created by accident.

Of course very few of these movies are considered classics or even particularly good within the horror genre, let alone the broader cinematic oeuvre. Technical and budget limitations (attempts to obscure sound dubbing problems in *The Beast of Yucca Flats* need to be seen to be believed), borderline acting, and implausible plots means many don’t age well. But that doesn’t mean that they are unimportant. They reflect the anxieties of their eras and warn of the timeless dangers of scientific hubris.

It is worth noting that while the zombie, loosely defined, has made a comeback in the 2000s, biology has superseded radiation as the mutagen; see, for example, the *Resident Evil* franchise (2002-2016), *28 Days Later/28 Weeks Later* (2002/2007), *Planet Terror* (2007), *Zombieland* and *Carriers* (2009), *World War Z* (2013) and *Extinction* (2015). However, one of the most significant findings of [a 2005 UN study](#) on the 1986 Chernobyl accident was that myths and misperceptions have resulted in “paralysing fatalism”—“negative self-assessments of health, belief in a shortened life expectancy, lack of initiative, and dependency on assistance from the state”—among residents in affected areas. While public understanding has improved, many of these fallacies and half-truths were reanimated with the Fukushima accident in 2011.

Although there are fewer nuclear weapons now than at the height of the Cold War, the risk of world-ending nuclear war remains. And regional instability, the proliferation of nuclear weapons and the materials to make them, and emerging global threats like cyber attacks and terrorism mean the risk of a single nuclear weapon or device being detonated—by accident, by miscalculation, or on purpose—is on the rise. While unlikely to enjoy a return to the halcyon B-movie years of the 1950s, the radioactive bogeyman likely has a long half-life.

Andrew Newman is Senior Director for Nuclear Fuel Cycle Activities at the Nuclear Threat Initiative (NTI). Prior to joining NTI, Newman worked at Harvard



CBRNE-TERRORISM NEWSLETTER – November 2017

*University's Project on Managing the Atom, the Australian Embassy's Nuclear Science and Technology Office in Washington, DC, the Russian-American Nuclear Security Advisory Council (now the Partnership for Global Security) in Washington, DC, and the Office of the Emergency Services Commissioner, Department of Justice, Victoria, Australia. Newman is an adjunct research associate at Monash University in Australia, where he holds a doctorate in political science and is the lead author of *Decision-making and Radioactive Waste Disposal* (Routledge, 2016). Andrew's first exposure to horror movies, courtesy of an older neighbor who screened many of the great late '70s/early '80s shockers (Halloween, Phantasm, Scanners, An American Werewolf in London) shortly after they were released on VHS, led to a lasting obsession with the genre.*

200 killed in tunnel collapse at North Korea nuclear test site

Source: <http://www.homelandsecuritynewswire.com/dr20171031-200-killed-in-tunnel-collapse-at-north-korea-nuclear-test-site>



A satellite image purportedly shows a North Korean nuclear test site Credit: EPA/AIRBUS / 38 NORTH / HANDOUT

Oct 31 – About 200 North Korean laborers and engineers have been killed after a mine shaft being dug at the country's nuclear test site collapsed in early September. On 3 September, North Korea conducted a nuclear test of a bomb with a yield of about 280 kilotons (the Hiroshima and Nagasaki bombs were in the 12-15 kiloton range). Experts say that the powerful test, conducted in a neighboring tunnel, may have weakened the wall- and ceiling-support scaffolding of the tunnel which collapsed. North Korea has conducted all its nuclear tests in a tunnel network under Mount Mantap. South Korean and Chinese scientists have warned that the mountain may be suffering from "Tired mountain syndrome," and that more tests may cause the mountain to collapse, releasing large amounts of radioactive fallout.

About 200 North Korean laborers and engineers have been killed after a mine shaft being dug at the country's nuclear test site collapsed, Japan's Asahi TV [reported](#).

The news channel quoted sources in North Korea who said that a tunnel being excavated by around 100 workers at the Punggye-ri test site collapsed earlier this month. An additional 100 workers sent to rescue the trapped laborers were killed when the tunnel suffered a second collapse.

Newsweek [reports](#) that the precise date for the disaster is not known, but that it occurred shortly after North Korea, on 3 September, conducted its sixth — and most powerful — underground nuclear test at the site.

Experts say that the powerful test, conducted in a neighboring tunnel, may have weakened the wall- and ceiling-support scaffolding of the tunnel which collapsed.



CBRNE-TERRORISM NEWSLETTER – November 2017

North Korea claimed that the 3 September test, which took place beneath Mount Mantap, was of a hydrogen bomb. Seismic sensors showed that the detonation was equivalent to an earthquake with a magnitude of 6.1 on the Richter scale. Analysts said the yield of the nuclear weapon detonated on 3 September was about 280 kilotons (the Hiroshima and Nagasaki bombs were in the 12-15 kiloton range). The seismic sensors which monitor North Korea's nuclear activity, also picked up the signs of underground collapses in the hours and days following the blast.



The *Telegraph* [reports](#) that satellite images of the Punggye-ri site, taken immediately after the test, showed considerable damage to surface features, including landslips. The damage is consistent with collapse of underground tunnels.

A study released 17 October by the [U.S.-Korea Institute](#) at Johns Hopkins University, and published on the [38 North](#) website, suggested the sixth underground test at the site had caused “substantial damage to the existing tunnel network under Mount Mantap.”

The study added that there is a possibility that the site is suffering “Tired mountain syndrome,” although there were no indications that it was being abandoned for future nuclear tests.

Newsweek notes that Nam Jae-chol, the director of South Korea's Meteorological Administration, warned in testimony before parliament on Monday that further tests at Punggye-ri could cause the mountain to collapse and release radioactivity into the environment.

“Based on our analysis of satellite imagery, we judge that there is a hollow space, which measures about 60 meters by 100 meters beneath Mount Matap,” he said. “Should another nuclear test take place, there is a possibility [of a collapse].”

Chinese scientists have issued similar warnings, saying that [nuclear fallout](#) could spread across “an entire hemisphere” if the mountain did collapse.



FAS Nuclear Notebook

Source: <https://fas.org/issues/nuclear-weapons/nuclear-notebook/>

The [FAS Nuclear Notebook](#) is co-authored by Hans M. Kristensen and Robert S. Norris and published bi-monthly in the *Bulletin of the Atomic Scientists*. Each issue provides a snapshot of a nuclear-armed country weapons programs or a global nuclear

weapons matter. The FAS Nuclear Notebook is one of the most widely sourced reference materials worldwide for reliable information about the status of nuclear weapons, and it is the most visited section of the [Bulletin of the Atomic Scientists web site](#). Because of their importance as a resource to an informed public debate about nuclear weapons, the FAS Nuclear Notebooks are freely available on the Internet.



CBRNE-TERRORISM NEWSLETTER – November 2017

The most recent FAS Nuclear Notebooks are listed below. Issues dating back to the very first issue in May 1987 [can be found here](#).

Recent FAS Nuclear Notebooks:

[November 2017: A history of U.S. nuclear weapons in South Korea.](#)

[September 2017: Worldwide deployments of nuclear weapons, 2017.](#)

May 2016: [no Notebook this month]

[March 2017: Russian Nuclear Forces, 2017](#)

[January 2017: United States Nuclear Forces, 2017](#)

[November 2016: Pakistani Nuclear Forces, 2016](#)

September 2016: [no Notebook this month]

[July 2016: Chinese Nuclear Forces, 2016](#)

[May 2016: Russian Nuclear Forces, 2016](#)

[March 2016: United States Nuclear Forces, 2016](#)

[January 2016: Declassified: US Nuclear Weapons at Sea During the Cold War](#)

Previous Nuclear Notebooks all the way back to the first issue in May 1987 [can be found here](#). The FAS Nuclear Notebook is currently produced by the analysts at the Federation of American Scientists. Previously it was produced by the Natural Resources Defense Council and called the NRDC Nuclear Notebook.

Israeli software gives New York power plants “Iron Dome” protection against failures

Source: <http://www.homelandsecuritynewswire.com/dr20171102-israeli-software-gives-new-york-power-plants-iron-dome-protection-against-failures>

Nov 02 – An Israeli company that developed the software for Israel's Iron Dome anti-missile system is working with the New York Power Authority to prevent unexpected shutdowns, *The Times of Israel* [reported](#) Sunday.

New York State Robert Moses Niagara Power Plant, Blenheim-Gilboa Pumped-Storage Power Plant, and a 500 MW plant in Queens now have software based on the software that runs Iron Dome.



New York Power Authority (NYPA) sought out **mPrest** after two of its largest transformers failed – the Blenheim-Gilboa Power Project in 2012 and Niagara Power Project two years later. Neither failure was catastrophic, but they cost more than \$5 million to repair.

NYPA presented its problem at a conference of the Israeli Smart Energy Association (ISEA), and mPrest suggested to NYPA that the software that runs Israel's

anti-missile Iron Dome system could be adapted for monitoring NYPA's power plants.

In 2015, the Israel-U.S. Binational Industrial R&D Foundation (BIRD) invested \$900,000 in the joint NYPA and mPrest project to develop the software. NYPA contributed \$975,000 to the project and mPrest about \$1.3 million.

The end result called the Asset Health Management application, or mNTCS monitors the status of the power plants. Using a combination of data gleaned from the transformer, information from various sensors, advanced algorithms and historical data, mNTCS shuts down equipment that is malfunctioning and reroutes the power to avoid unplanned shutdowns. This proactive approach reduces the chances of an explosion due to a malfunction, protects workers and saves NYPA money.



While the software can't prevent shutdowns due to extreme external conditions—such as hurricanes or earthquakes—it can analyze what caused a problem after the fact.

The mPrest software, which is an example of how Israeli companies leverage military technology for civilian use, may soon be used in other locations in the United States, as well as in Australia, New Zealand, Latin America, China, and Europe, according to Doron Gover, a retired Israel Air Force pilot now in charge of corporate development for mPrest.

Vector, the largest power distributor in New Zealand, invested \$10 million in mPrest, Reuters reported on Monday. Vector will be the second largest shareholder in mPrest, following just Rafael Advanced Defense Systems, an Israeli state-owned defense contractor. The software will be used to provide power to Auckland's 1.4 million residents. According to Vector Chairman Michael Stiasny, the company hopes that the software will also allow the company to sell excess power to other localities in New Zealand and even in Australia in the future.

Nuclear energy programs do not increase likelihood of nuclear weapons proliferation: Study

Source: <http://www.homelandsecuritynewswire.com/dr20171106-nuclear-energy-programs-do-not-increase-likelihood-of-nuclear-weapons-proliferation-study>

Nov 06 – Contrary to popular thought, nuclear proliferation is not more likely to occur among countries with nuclear energy programs, according to research published in [International](#)

nuclear energy programs. Moreover, countries that pursued nuclear weapons under the cover of an energy program have not been significantly more likely to acquire nuclear weapons, when compared to countries that seek nuclear weapons without an energy program.

As the study points out, nuclear energy programs do provide an increased technical ability to develop nuclear weapons. However, countries with nuclear energy programs face political obstacles that help counter this proliferation risk, including improved intelligence by outside actors, and the prospect of costly nonproliferation sanctions, which jeopardize the international trade and supplies required for most

energy programs to operate. When a country announces plans to develop nuclear energy, this provides an open signal for foreign intelligence agencies to pay closer attention. As nuclear energy programs become operational, the procurement of technology and materials from foreign firms provide these same agencies with opportunities for surveillance, increasing the likelihood that suspicious activities are detected in a timely fashion. Furthermore, given that the nuclear power plant industry relies on a small number of global suppliers, nearly all of whom require International Atomic Energy Agency safeguards and



Security.

In a historical analysis of the relationship between nuclear energy programs and proliferation from 1954 to 2000, the study finds that the link between the two has been overstated. Out of more than fifteen countries that have pursued nuclear weapons since the first nuclear power reactor came online in the 1950s, only five — Argentina, Brazil, India, Iran, and Pakistan — began pursuing nuclear weapons after a nuclear energy program had already been initiated. Most countries either pursued nuclear weapons following a more covert approach or had already begun seeking nuclear weapons before they had started



CBRNE-TERRORISM NEWSLETTER – November 2017

the peaceful use of exported materials, countries with energy programs are generally wary of risking disruptions in supply by seeking to develop nuclear weapons.

“The findings suggest that international efforts to manage the proliferation risks of nuclear energy programs have been quite effective,” [says](#) author Nicholas L. Miller, assistant professor of government at Dartmouth. “Even when countries become more technically capable of developing nuclear weapons due to an energy program, they can often be restrained by timely intelligence and the prospect of sanctions.”

In the past, the U.S. has helped advance and enforce nonproliferation by leveraging its role as a major supplier of nuclear power plants and enriched uranium fuel. This leverage has diminished in recent years, as the U.S. is now only a marginal supplier in a nuclear export market dominated by Russia, with China also

aiming to increase its share. To restore this important leverage, Miller proposes that the U.S. work to revive its role as a major nuclear supplier.

For nuclear cooperation agreements, Miller calls on the U.S. to forego a demand for the “gold standard” in which recipient countries must pledge not to pursue enrichment or reprocessing. This stringent requirement may scare off potential buyers, who then take their business elsewhere, which in turn reduces the United States’ potential for leverage. While the U.S. should continue to oppose the spread of enrichment or reprocessing technology, it can pursue this objective via more effective strategies, such as consultations with other nuclear suppliers and quiet but forceful diplomacy with countries attempting to acquire this sensitive technology.

— *Read more in Nicholas Miller, “Why Nuclear Energy Programs Rarely Lead to Proliferation,” [International Security](#) 42, no. 2 (Fall 2017): 40-77.*

EDITOR’S COMMENT: And what about Turkey’s nuclear ambitions???

Staying “PRIMED” for a Radiation Event

By Grant Coffey

Source: <https://www.domesticpreparedness.com/healthcare/staying-primed-for-a-radiation-event/>

Nov 08 – Chemical, biological, radiological, nuclear, and explosive (CBRNE) events are low in frequency, but high in consequence, requiring a frequent and more targeted emphasis on the way that responders train and learn. Radiation is often not well understood. It can be intimidating for both the public and for first responders. Radiation cannot be seen, smelled, or heard. Yet, risk is relatively easy to mitigate when responders have been adequately trained and equipped.

A Six-Step Training Checklist

Prepare. Radiation events can be overwhelming and chaotic. Preparation must be done before the event and should be based on best practices. Meetings and trainings with support agencies like local state radiation regulatory agencies, [Civil Support Teams](#), and Radiological Assistance Program teams should occur before the need arises. This sets a critical foundation in a successful working relationship: responders arriving on scene can integrate with radiation officials to work quickly and effectively. A radiation specialist from the closest hazmat response team can be an effective resource, so it is important to build rapport and cross-team familiarization with local hazardous materials response teams.

Recognize. Upon arriving on scene, responders should check-in with incident command and perform a quick situational assessment. Rushing in before recognizing hazard zones and personal protective equipment (PPE) requirements is dangerous. Basic recognition of the scene type and scope of the incident can prevent a minor scene from becoming a catastrophe. It is imperative to recognize the possibility of the presence of radiation.

Input. Identify scene “cues and clues.” These are important pieces of the much larger incident picture. Ionizing radiation can be anywhere within a community. Knowing what type it is and where it is helps responders to develop a safe and effective plan. There are four basic categories of ionizing radiation: naturally occurring radioactive material, industrial,



CBRNE-TERRORISM NEWSLETTER – November 2017

medical, and special nuclear material. Understanding where each of these types of radiation are located in the community helps responders quickly recognize anything unusual, which should raise suspicion. One key input item here is an explosion with an unidentified source. In this case, the possibility of radiation should be suspected. Once radiation is ruled out, responders can then proceed with other scene priorities.

Monitor. Responders to a CBRNE incident must be able to assess radiation levels, verify radiation boundaries, define contamination areas, and, when possible, attempt to identify specific radionuclides. This could be a critical piece of information in the attempt to determine whether an event is accidental or intentional. It is important to remember that equipment provides only a partial assessment and is only as good as the knowledge and skill of the user.

Experience. Ultimately, the brain is the best tool in the field. Experience is vital, but should be based on tested operational truths from other events and then learned. Only then can this experience be integrated into daily response habits. This is especially critical when dealing with radioactivity because there are few incidents to learn from.

Decision. The final but perhaps most important step in the PRIMED process is making a decision. Radiation incidents, though overwhelming, have common patterns. If these patterns are recognized early, they can help pave the way to safer decision making under stress. Radiation is a predictable physical phenomenon, which can be used to a responder's advantage.

Although radiation is naturally occurring energy, responders should strive to avoid any additional amount of ionizing radiation. Once it has been determined that radiation is present, responders must keep exposure or dose of radiation to a minimum by observing ALARA, which stands for "As Low As Reasonably Achievable." This term refers to radiation exposure and reminds responders to always pay attention to personal safety. ALARA is a regulatory requirement but, aside from that, ionizing radiation is still a major health and safety hazard. Without applying the principles of ALARA, a worker who is continually exposed to ionizing radiation can receive irreversible cell damage, which can manifest in harmful ways (e.g., increased risk for cancer, genetic mutations, organ failure, and even death).

In addition to practicing ALARA, it is critical that first responders use appropriate PPE when responding to a radiation incident. Three factors should be considered for minimizing the effects of radiation exposure:

- ◆ **Time** – Responders should spend as little time as possible in a radiation field to minimize dose.
- ◆ **Distance** – Responders should put distance between them and the source. Further distance from a radiation source means less exposure.
- ◆ **Shielding** – Responders should wear appropriate PPE (including respiratory protection) and keep dense materials between them and the radiation field. [Ionizing radiation](#) exists in the form of energy (x-rays, gamma rays) and sub-atomic particles (alpha and beta particles). High-density materials such as lead and thick steel or concrete can provide some shielding from the high-energy waveform of ionizing radiation, though generally not practical on an emergency scene.

The essential point is that responders must observe ALARA during radiation events and always remember radiation rule #1: "Turn it on and put it on." A personal radiation-monitoring device (PRD) is critical to alert responders to the presence of radiation. PRDs are important tools that can save lives by alerting responders when they have entered a significant radiation field or have accumulated a significant dose of radiation. Good education and field guides based on operationally tested factors are key to helping organize on-scene priorities. Radiation safety is of the utmost importance. By following the principles from the PRIMED training checklist and heeding the protection mantra ALARA, responders can minimize their risk of radiation exposure.

Grant Coffey is a retired Portland Fire & Rescue Hazmat Team coordinator, College Fire Science instructor, and chemical, biological, radiological, nuclear, and high-yield explosive (CBRNE) expert of nearly 40 years. He trains fire, police, military, and industry hazmat responders. He has National Fire Protection Association (NFPA) certifications for radiation specialist and is a state of Oregon radiation safety officer. He is also a hazmat specialist and incident safety officer and has experience in emergency management and various other CBRNE hazmat disciplines. He hosts CBRNE response training videos online at FLIR.com/PRIMED.



RanidSOLO

**Spectrometric Radiation Source
Locator for RanidPro200**



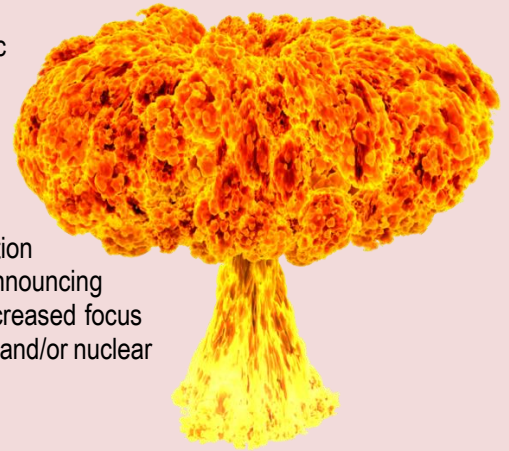
- ✓ High precision automated localization method
- ✓ Calculation of the radiation source direction
- ✓ Exceeds ANSI and IEC standard (15 degrees precision)
- ✓ Estimation of the source location calculated reliably and quickly – approx. 12 sec
- ✓ Possibility to extend the measurement network with several units to gain better situational overview
- ✓ Full CBRN extendibility

Preparedness Goals Associated with the Nuclear Threat

By Vayl Oxford

Source: <http://www.domesticpreparedness.com/commentary/final-report-preparedness-goals-associated-with-the-nuclear-threat/>

Nov 08 – A nuclear attack on U.S. soil is possibly the most catastrophic threat facing the nation, which is why it has been at the top of the national security agenda for the last two administrations. President George W. Bush espoused a strategy based on a layered defense involving: increased efforts to secure and reduce nuclear material and stockpiles globally; increased efforts to counter nuclear smuggling through the Proliferation Security Initiative in 2003; enhanced international cooperation by expanding the 1991 Cooperative Threat Reduction Program and announcing the 2006 Global Initiative to Combat Nuclear Terrorism; and, finally, increased focus on domestic measures to protect the United States against a radiological and/or nuclear (R/N) attack.



U.S. Initiatives to Guard Against Nuclear Attacks

In 2005, President Bush issued National Security Presidential Directive-43, and Homeland Security Presidential Directive-14, to establish the Domestic Nuclear Detection Office (DNDO) within the Department of Homeland Security (DHS). DNDO's principal goals are to:

- Develop an enhanced domestic system to detect, and report attempts to import or use, R/N materials/weapons in the United States;
- Enhance and coordinate nuclear detection efforts of federal, state, and local governments;
- Establish procedures needed to ensure that detection leads to effective response;
- Develop an enhanced Global Nuclear Detection Architecture; and
- Support the effective sharing of appropriate information.

President Barack Obama has built upon this strategy, while putting additional emphasis on reducing the threat, through the Global Nuclear Lockdown program and the New Strategic Arms Reduction Treaty (START) with Russia. START further reduces the U.S. and Russian nuclear stockpiles.

Despite these concerted efforts, there are continuing concerns that the nuclear threat is growing. The Commission on the Prevention of WMD (Weapons of Mass Destruction) Proliferation and Terrorism echoed this concern in its "World at Risk" report, which stated the following:

"The number of states that are armed with nuclear weapons or are seeking to develop them is increasing. Terrorist organizations are intent on acquiring nuclear weapons or the material and expertise needed to build them. Trafficking in nuclear materials and technology is a serious, relentless, and multidimensional problem. ... [T]he Commission was unanimous in concluding that the nuclear aspirations of Iran and North Korea pose immediate and urgent threats to the Nuclear Nonproliferation Treaty. Successful nuclear programs in both countries could trigger a cascade of proliferation."

Since the Commission's report, activities in both of these nations reinforce the need for increased concern about their intentions and capabilities. With respect to Iran, assessments emanating from the International Atom Energy Agency's (IAEA) inspections include:

- Operations at the deep underground enrichment facility near Qom;
- Uranium enrichment at the highest rate ever – i.e., 3.5 percent;
- Quantity of centrifuges operating in Natanz at a new high – with more than 5,000 yet to be installed;
- Production of enriched uranium at the fastest rate ever – i.e., 20 percent;
- Decreased amount of time needed to produce enough fissile material for a nuclear weapon, which could produce enough material for a weapon in 43 days (dropping to 11 days by February 2013 if 20-percent enrichment rate continues).

These revelations, along with Iran's stated objectives and ties to terrorist groups, serve as a clear signal that the United States needs a multi-faceted strategy to prevent Iran from crossing the nuclear threshold, while also recognizing that it may very well reach nuclear weapons state status. Meanwhile, North Korea continues to defy the international community with its missile launches and reported plans to conduct an additional underground nuclear test.



CBRNE-TERRORISM NEWSLETTER – November 2017

The Commission also cites that Pakistan poses a particular concern because of: (a) its own stockpile of nuclear weapons; and (b) the active presence of al-Qaida within its borders. Insights that came to light following the killing of Osama Bin Laden raise additional concerns about the nexus of terrorism with a nuclear armed state. Moreover, the recent nuclear crisis in Japan provides even more evidence that nuclear-related events require consideration of all-hazard approaches to threat response. Concerns about medical countermeasures arise after an R/N threat is acknowledged, and those concerns will require the public health community to be involved in managing the response even before an attack is officially launched.

Against this backdrop, DomPrep surveyed its readers regarding: (a) the current state of U.S. preparedness to defend against an R/N attack; and (b) steps that might and/or should be taken to improve preparedness.

Key Findings

- ◆ More than half of the respondents agreed that developing a domestic layer of the Global Nuclear Detection Architecture serves as an effective tool in preventing an R/N attack. Interestingly, almost one-third were unsure about its effectiveness possibly due to limited exposure to the goals of the architecture or a serious concern about its utility.
- ◆ More than three-quarters of the respondents felt that current federal government efforts to increase preparedness of major U.S. cities were not adequate to protect against an R/N attack.
- ◆ Regarding the responsibility and means to develop capabilities and capacities to prevent an R/N attack, an overwhelming number of respondents feel that it is a shared responsibility among federal, state, and local governments. On the other hand, less than one-fifth felt the DHS-managed grant process was an effective approach to build capabilities and capacities.
- ◆ Nearly all of the respondents felt that integration across the federal government, law enforcement, and emergency response communities to react to a possible R/N threat is minimal or only exists in certain communities.
- ◆ More than three-quarters of the respondents agreed that exercises and training were very important to improving preparedness and response capabilities, and they should be routinely conducted at the state and local level with support from the federal government.

[Click to download Full Report](#)

Vayl Oxford assumed the position of National Security Executive Policy Advisor at the Pacific Northwest National Laboratory (PNNL) as of 1 May 2012. He is the former Director of the Department of Homeland Security's (DHS) Domestic Nuclear Detection Office (DNDO). Prior to DHS, he was the Special Assistant for Policy Planning in the DHS Science and Technology Directorate and Acting Director of the Homeland Security Advance Research Projects Agency. At the Department of Defense, he was the Deputy Director of technology development at the Defense Threat Reduction Agency (DTRA) and Chief of counter-proliferation programs at the Defense Special Weapons Agency/Defense Nuclear Agency.

Mysterious Radioactive Cloud Over Europe Hints At Accident Farther East

Source: <https://www.npr.org/sections/thetwo-way/2017/11/10/563286253/mysterious-radioactive-cloud-over-europe-hints-at-accident-farther-east>

Nov 10 – European authorities are providing new details about a cloud of mysterious radioactive material that appeared over the continent last month.

Monitors in Italy were among first to detect the radioactive isotope ruthenium-106 on Oct. 3, according to [a fresh report](#) by France's [Radioprotection and Nuclear Safety Institute](#), known as IRSN. In total, 28 European countries saw the radioactive cloud, the report says.





Monitoring stations similar to this one in Germany detected unusual radioactive material over Europe last month.

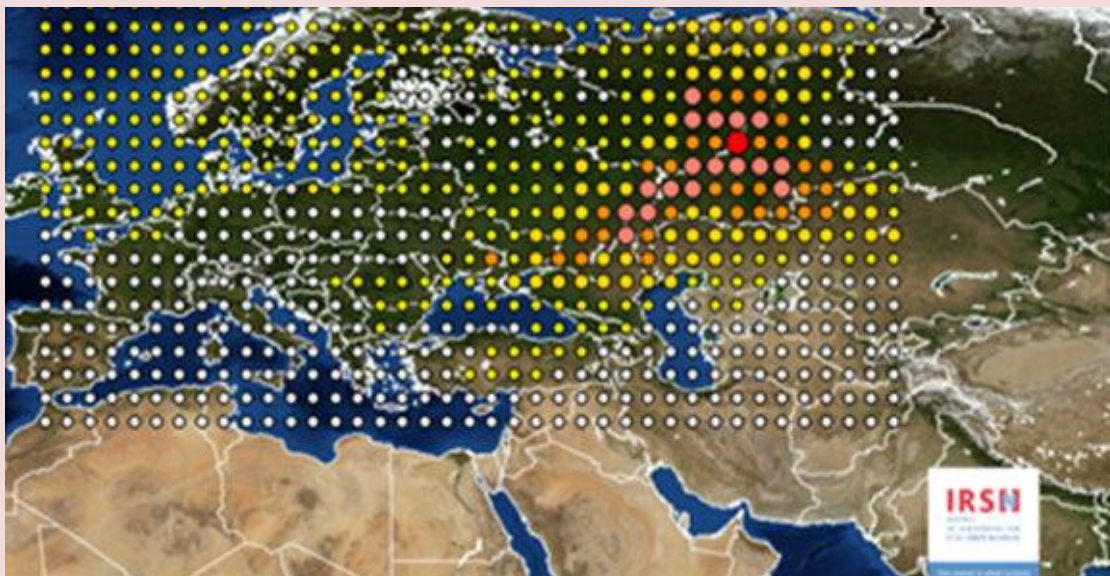
The multinational [Comprehensive Nuclear-Test-Ban Treaty Organisation](#), which runs a network designed to monitor for nuclear weapons tests, also confirmed to NPR that it had detected the cloud.

Based on the detection from monitoring stations and meteorological data, the mysterious cloud — which has since dissipated — has been traced to somewhere along the Russia-Kazakhstan border,

according to Jean-Christophe Gariel, director for health at the IRSN.

"It's somewhere in South Russia," he says, likely between the Volga River and the Ural Mountains.

Authorities say the amount of material seen in Europe was small. "It's a very low level of radioactivity and it poses no problems for health and the environment in Europe," Gariel says.



A map from French authorities suggests that the release came from the east, near the border of Russia and Kazakhstan.

But modeling suggests that any people within a few kilometers of the release — wherever it occurred — would have needed to seek shelter to protect themselves from possible radiation exposure.

"If it would have happened in France, we would have taken measures to protect the population in a radius of a few kilometers," Gariel says. French authorities, he adds, will conduct random checks of foodstuffs from the region to check for possible contamination of agricultural products.

Ruthenium-106 is a radioactive isotope that is not found in nature. "It's an unusual isotope," says Anders Ringbom, the research director of the [Swedish Defence Research Agency](#), which runs radioactive monitoring for that nation. "I don't think we have seen it since the Chernobyl accident."

The IRSN analysis suggests that the ruthenium did not come from a nuclear reactor accident. Instead, it most likely came from either the chemical reprocessing of old nuclear fuel or the production of isotopes used in medicine. Based on the size of the release, Gariel says, whatever happened had to have been accidental.

"It's not an authorized release, we are sure about that," he says.

A handful of Russian nuclear facilities are located roughly in the region where the ruthenium originated, including a large nuclear reprocessing plant known as the [Mayak Production Association](#).



CBRNE-TERRORISM NEWSLETTER – November 2017

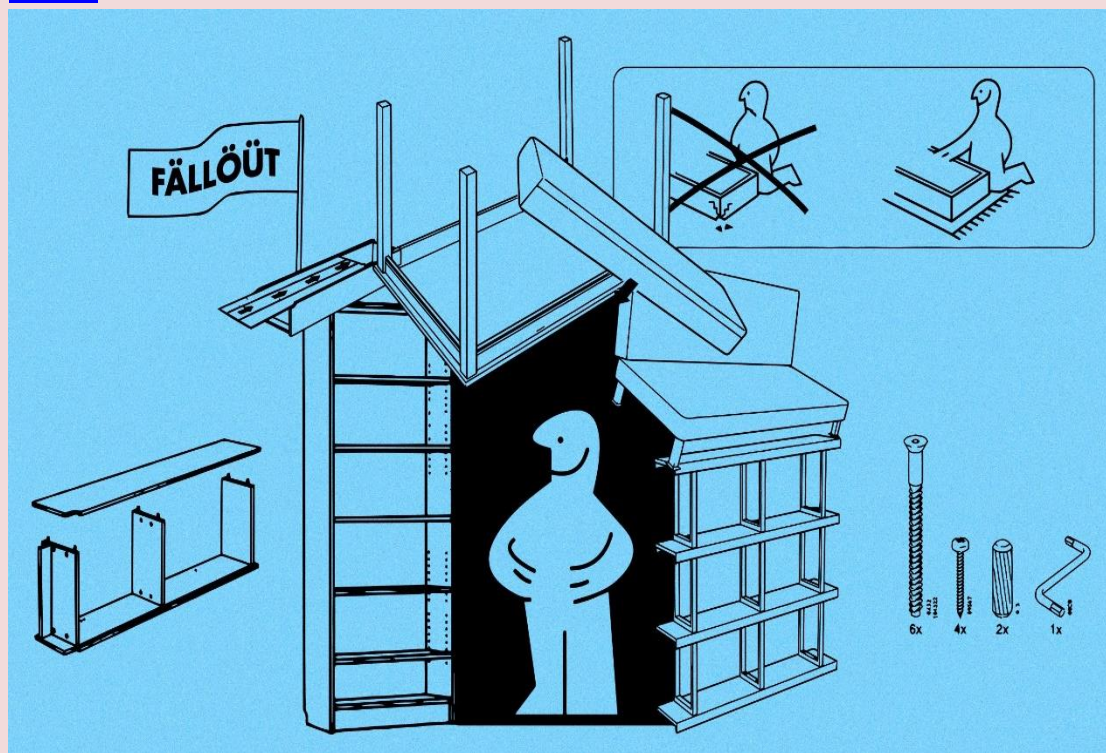
During the Cold War, the Mayak plant turned used nuclear fuel into material for nuclear weapons. The plant has been the site of numerous past accidents, including a 1957 explosion that rivaled the nuclear meltdowns at Fukushima and Chernobyl.

Gariel says that while Mayak is a possible source of the cloud, there simply aren't enough data to conclusively link it to the release of radioactive material. He also says he has spoken to Russian safety officials over the past few days and that while they do not dispute his analysis, they are unaware of any incidents in the region in the past few months.

*Science editor **Geoff Brumfiel** oversees coverage of everything from butterflies to black holes across NPR News programs and on NPR.org. Prior to becoming the editor for fundamental research news in April of 2016, Brumfiel worked for three years as a reporter covering physics and space. Brumfiel has carried his microphone into ghost villages created by the Fukushima nuclear accident in Japan. He's tracked the journey of highly enriched uranium as it was shipped out of Poland. For a story on how animals drink, he crouched for over an hour and tried to convince his neighbor's cat to lap a bowl of milk. Before NPR, Brumfiel was based in London as a senior reporter for Nature Magazine from 2007-2013. There he covered energy, space, climate, and the physical sciences. In addition to reporting, he was a member of the award-winning Nature podcast team. From 2002 – 2007, Brumfiel was Nature Magazine's Washington Correspondent, reporting on Congress, the Bush administration, NASA, and the National Science Foundation, as well as the Departments of Energy and Defense.*

How to Build a Fallout Shelter Using Nothing but IKEA Furniture

Source: https://www.vice.com/en_us/article/kz3pda/how-to-build-a-fallout-shelter-using-nothing-but-ikea-furniture



Nov 10 – "Obviously, real wood would be better. But that's better than nothing," an expert in disaster preparedness told me.

►► Read more at source's URL.





HOTZONE[®]
SOLUTIONS

Tel: +31(0)70 262 97 04

sales@hotzonesolutions.com

SEA BASED RADIATION EARLY WARNING SYSTEM

Hotzone Solutions, with its partners, MOBILIS/France and GIHMM/ Austria, offers a complete solution, based on special radiation detectors mounted on a range of data buoys. These SBREWS can be installed at any sea-based location on the globe. SBREWS are designed to measure and IDENTIFY radioactivity of gamma radiation. Its wide measuring range permits the detection of minor changes in the ambient natural radioactivity as well as measuring and identifying – spectroscopic monitoring – high dosage rates. Aerosol sampling can be integrated upon request.



Russia Is Preparing for a Nuclear or Chemical Attack as Tensions With NATO Build

Source: <http://www.newsweek.com/russian-forces-prepare-nuclear-attack-south-regions-709286>

Nov 13 – **Russian troops near the Black Sea coast have carried out drills for a scenario in which Russia was attacked by a chemical or nuclear weapon, the country's military has revealed.**

Spread across three Russian regions between the Black and Caspian seas, the drills involved more than 5,000 troops, the Ministry of Defense announced in a [statement](#) Monday.

Preparing for a scenario in which Russia was attacked by “weapons of mass destruction by a hypothetical enemy,” soldiers were deployed in hazmat suits and gas masks.

Units specializing in chemical weapons were deployed in the Krasnodar and Stavropol regions, while at least 100 personnel in the neighboring Rostov region launched a parallel decontamination drill on Monday. It followed similar exercises held by Russian overseas troops [in nearby Armenia over the weekend](#).



Cadets wear gas masks as they take part in exercises at Serpukhov Military Institute of Rocket Forces in Serpukhov town, 100 kilometers (62 miles) south of Moscow, on April 6, 2010. Denis Sinyakov/Reuters

Also deployed were mobile laboratories and radioactive- and chemical-tracing reconnaissance vehicles capable of quarantining, assessing and potentially eliminating a chemical or nuclear threat.

In recent weeks, Russia's nuclear-capable forces practiced missile [launches and flyovers in apparent offensive measures](#) for a conflict scenario. The military has pledged to test its Sarmat intercontinental ballistic missile system before the end of the year.

Russian Minister of Defense Sergei Shoigu has alleged that NATO is [developing use of nuclear arms near](#) Russia's western borders last week, but has not provided evidence for the claims.

Russian President Vladimir Putin has repeatedly warned of the dangers of a nuclear conflict, mostly in response to the growing rift between the West and his government.

Russia's annexation of Crimea, backing of separatist insurgents in Ukraine's east and its military support for Syrian President Bashar al-Assad have been the major sticking points that have worsened ties with the U.S. and European states.

Recent allegations that Russia interfered in the U.S. presidential election last year have halted Trump's campaign initiative to reach out to Putin and improve relations.



CBRNE-TERRORISM NEWSLETTER – November 2017

While a handful of officials have made a habit of speaking about hypothetical massive and possibly nuclear conflict, opinion polls show the majority of Russians are wary to believe such a scenario is likely, despite the rift with the West.

According to state pollster [WCIOM](#), 63 percent of Russians felt that war with the U.S. or NATO was impossible or unlikely in April. Although North Korea enjoys a better relationship with Russia than with most countries, the country's nuclear weapons program was [viewed as a threat](#) by 67 percent of Russians. A total of 39 percent believed North Korea directly threatened Russia.

EDITOR'S COMMENT: Does this mean that we in Europe still have chemical weapons? Interesting! I know that our allies over the ocean do have some under destruction but...

RanidSOLO

Spectrometric Radiation Source Locator for RanidPro200

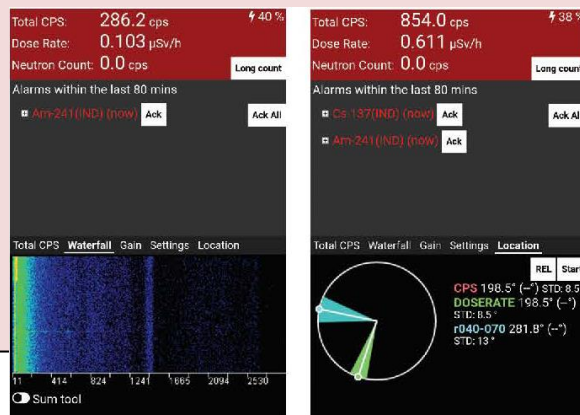
Source: <https://www.environics.fi/product/ranidsolo/>

RanidSOLO is an efficient and innovative device that bridges the “missing link” of radiation source localization in field operations. Its high precision automated method is able to calculate the estimated location direction of one or multiple radiation sources in a short time frame of approx. 12 seconds.

Smartphone application

The results from the measurements done in the field can be checked immediately in loco by the operators (on the smartphone / toughpad display) or can be collected and analysed together by the command centre.

This highly sensitive equipment is based on LaBr₃, 1.5"x1.5" LaBr₃ scintillator with an automated rotating attenuator, detects gamma



radiation and provides the direction towards the source, when combined to a small rotating attenuator. This component acts as a small shield that reduces the signal and creates the cone “pointing” to the estimated source direction. The automated localization method can achieve a high precision (a few degrees).



Key features

- High precision automated localization method
- Calculation of the radiation source direction
- Exceeds ANSI and IEC standard (15 degrees precision)
- Estimation of the source location calculated reliably and quickly – approx. 12 sec
- Possibility to extend the measurement network with several units to gain better situational overview
- Full CBRN extendibility

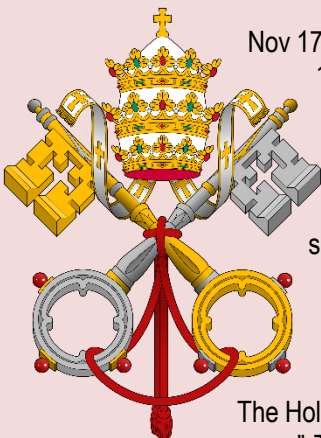
Main application areas

- Border CBRN Monitoring
- Building CBRN Monitoring
- Armoured CBRN Reconnaissance
- Light CBRN Reconnaissance
- Mass Events



What does the Church really teach about nuclear war?

Source: <https://www.catholicnewsagency.com/news/what-does-the-church-really-teach-about-nuclear-war-23759>



Nov 17 – A Vatican conference discussing “A World Free From Nuclear Weapons,” held Nov. 10-11, is the latest step in a long-term commitment from the Holy See to work for nuclear disarmament, which itself is considered by the Vatican to be a step toward the goal of integral disarmament.

The conference was held after 120 nations voted this July to pass the UN's Comprehensive Treaty on the Prohibition of Nuclear Weapons. The treaty prohibits signatories from developing, testing, producing, manufacturing, acquiring, possessing or stockpiling nuclear weapons or other nuclear explosive devices, and prevents them from using these weapons. To date, only three countries have ratified the treaty.

The Holy See actively took part in the treaty's negotiations, and is among the three nations that have ratified the treaty

The Holy See has a “Permanent Observer” status at the United Nations, although with “enhanced powers.” That means that the Holy See can take part in the negotiations of treaties, but does not usually have the right to vote.

For the July 7 vote on the nuclear treaty, the Holy See was accepted by the UN to participate in negotiations as a full member, and was permitted to vote on the matter before the adoption of the treaty. This was the first time the Holy See has been afforded such a status at the UN, which Archbishop Paul Richard Gallagher, the Vatican's “foreign minister,” described as a milestone during the treaties ratification ceremony Sep. 20.

This diplomatic initiative shows the strength of the Holy See's commitment to nuclear disarmament.

In fact, the Holy See has understood for decades the perilous potential of nuclear weaponry.

During the Second World War, Pius XII understood that new scientific developments could be used to produce weapons of mass destruction.

Pope Pius XII's concerns were expressed in three different speeches delivered at the Pontifical Academy for Sciences between 1941 and 1948.

Talking on Nov. 30, 1941, Pius XII said in the hands of men, science can be a double edged weapon, able to heal and kill at the same time. The Pope also said that he was following “the incredible adventure of the men committed to research on nuclear energy and nuclear transformation” thanks to Max Planck, Nobel Prize Laureate in 1918, who served as member of the Pontifical Academy for Sciences.

Pope Pius XII warned about nuclear danger again, in a meeting with members of the Pontifical Academy that took place Feb. 21, 1943. On that occasion, the Pope warned that



CBRNE-TERRORISM NEWSLETTER – November 2017

because of the development of nuclear weapons, “there could be a dangerous catastrophe for our planet as a whole.”

Finally, in a speech delivered to the Pontifical Academy for Science on Feb. 8, 1948, the Pope talked about the atomic bomb as one of the “most horrible weapons the human mind has ever conceived,” and asked: “What disaster should the humanity expect from a future conflict, if stopping or slowing the use of always more and more surprising scientific inventions would be proven impossible? We should distrust any science whose main goal is not love.”

Like Pius XII, St. John XXIII urged the need for an “integral disarmament” in his encyclical *Pacem In Terris*, and the Second Vatican Council’s Apostolic Constitution *Gaudium et Spes* stressed that “power of weapons does not legitimate their military and political use.”

Speaking at the UNESCO June 2, 1980, Pope St. John Paul II explicitly mentioned the “nuclear threat” on the world that could lead to “the destruction of fruits of culture, products of the civilization built in centuries by generation of men who believed in the primacy of the spirit and did not spare efforts nor fatigues.”



John Paul II noted the “fragile balance” of the world, caused by geopolitical reasons, economic problems and political misunderstandings along with wounded national prides. But, he said, this balance can be destroyed at any moment, following “a mistake in judging, informing, interpreting.”

He then asked: “Can we still be certain that breaking the balance would not lead to war and to a war that would not hesitate to use nuclear weapons?”

Benedict XVI also confronted the issue many times. It is especially noteworthy to recall what Benedict said in his May 31, 2009 Pentecost homily.

Benedict XVI stressed that “man does not want to be in the image of God any longer, but only in his own image: he declares himself autonomous, free.”

A man in such an “unauthentic relation” with God can become dangerous, and “can revolt against life and humanity,” as the Hiroshima and Nagasaki tragedies showed, the Pope said.

Pope Francis has warned many times about the risks of the nuclear proliferation. In a message sent to the UN Conference for the Negotiation of the Treaty for the Prohibition of Nuclear Weapons, Pope Francis stressed that “International peace and stability cannot be based on a false sense of security, on the threat of mutual destruction or total annihilation, or on simply maintaining a balance of power.”

“We need – he added - to go beyond nuclear deterrence: the international community is called upon to adopt forward-looking strategies to promote the goal of peace and stability and to avoid short-sighted approaches to the problems surrounding national and international security”.

The Holy See has followed a clear path on nuclear disarmament, which it continued with this month’s conference. The words of Pope Francis at the conference carry the legacy and tradition of the Church’s teachings on nuclear weaponry and its danger.

We can not “fail to be genuinely concerned by the catastrophic humanitarian and environmental effects of any employment of nuclear devices,” the Pope said.

“If we also take into account the risk of an accidental detonation as a result of error of any kind, the threat of their use, as well as their very possession, is to be firmly condemned. For they exist in the service of a mentality of fear that affects not only the parties in conflict but the entire human race. International relations cannot be held captive to military force, mutual intimidation, and the parading of stockpiles of arms. Weapons of mass destruction,



particularly nuclear weapons, create nothing but a false sense of security. They cannot constitute the basis for peaceful coexistence between members of the human family."

New theory of the opening moments of Chernobyl disaster

Source: <http://www.homelandsecuritynewswire.com/dr20171120-new-theory-of-the-opening-moments-of-chernobyl-disaster>



Nov 20 – A new theory of the opening moments during the Chernobyl disaster, the most severe nuclear accident in history, based on additional analysis is presented for the first time in the journal [Nuclear Technology](#), an official journal of the American Nuclear Society. The new theory suggests the first of the two explosions reported by eyewitnesses was a nuclear and not a steam explosion, as is currently widely thought and is presented by researchers from the Swedish Defense Research Agency, Swedish Meteorological and Hydrological Institute, and Stockholm University.

They hypothesize that the first explosive event was a jet of debris ejected to very high altitudes by a series of nuclear explosions within the reactor. This was followed, within three seconds, by a steam explosion which ruptured the reactor and sent further debris into the atmosphere at lower altitudes.

T&F [says](#) that the theory is based on new analysis of xenon isotopes detected by scientists from the V.vG. Khlopin Radium Institute in the Leningrad, four days after the accident, at Cherepovets, a city north of Moscow far from the major track of Chernobyl debris. These isotopes were the product of recent nuclear fission, suggesting they could be the result of a recent nuclear explosion. In contrast, the main Chernobyl debris which tracked northwest to Scandinavia contained equilibrium xenon isotopes from the reactor's core.

By assessing the weather conditions across the region at the time, the authors also established that the fresh xenon isotopes at Cherepovets were the result of debris injected into far higher altitudes than the debris from the reactor rupture which drifted towards Scandinavia.

Observations of the destroyed reactor tank indicated that the first explosion caused temperatures high enough to melt a two-meter thick bottom plate in part of the core. Such damage is consistent with a nuclear explosion. In the rest of the core, the bottom plate was relatively intact, though it had dropped by nearly four meters. This suggests a steam explosion which did not create temperatures high enough to melt the plate but generated sufficient pressure to push it down.

Lead author and retired nuclear physicist from the Swedish Defense Research Agency, Lars-Erik De Geer commented, "We believe that thermal neutron mediated nuclear explosions at



CBRNE-TERRORISM NEWSLETTER – November 2017

the bottom of a number of fuel channels in the reactor caused a jet of debris to shoot upwards through the refueling tubes. This jet then rammed the tubes' 350kg plugs, continued through the roof and travelled into the atmosphere to altitudes of 2.5-3km where the weather conditions provided a route to Cherepovets. The steam explosion which ruptured the reactor vessel occurred some 2.7 seconds later." Seismic measurements and an eye-witness report of a blue flash above the reactor a few seconds after the first explosion also support the new hypothesis of a nuclear explosion followed by a steam explosion. This new analysis brings insight into the disaster, and may potentially prove useful in preventing future similar incidents from occurring.

— Read more in Lars-Erik De Gerr et al., "A Nuclear Jet at Chernobyl Around 21:23:45 UTC on April 25, 1986," [Nuclear Technology](#) (16 November 2017).



ICI
International
CBRNE
INSTITUTE



EXPLOSIVE NEWS



The Pentagon's IED-Hunters Have a New Target: Drones

Source: <http://www.defenseone.com/threats/2017/10/pentagons-ied-hunters-have-new-target-drones/142051/>

Man behind Greek parcel bombs



Malta's explosive history: 19 bomb attacks since 2010

Malta has experienced 19 bomb attacks since 2010, with five people targeted in the last 11 months. Several of these cases are still unsolved, with many cases linked to diesel smuggling, drug trafficking and usury.

Source: http://www.maltatoday.com.mt/news/national/81438/maltas_explosive_history_19_bomb_attacks_since_2010#.WfmVHHb-vlV

Oct 19 – This week, Malta has been left in shock after the news of journalist Daphne Caruana Galizia's murder. A bomb was detonated in Caruana Galizia's rental car close to her house last Monday. Although the event marks the first time a journalist has been killed, targeting people with explosives is no new concept in Malta.



Daphne Caruana Galizia is the third victim of explosive devices in 2017, and the fifth person to die since 2010. Although explosive devices such as car bombs are on the rise, with more people being targeted each year, most of these cases have not been solved and no action has been taken.

The most recent attack happened on **20 February 2017**, when a

device was detonated in 40-year-old [Romeo Bone](#)'s car. Bone, who was well known to police, lost both legs in the incident but survived.





Romeo Bone lost both his legs in a car bomb

On 29 January 2017, [Victor Calleja](#), 61, died when a bomb detonated in his car in Marsa. The bomb was

believed to have been detonated electronically. Calleja, known as Ic-Chippu, was also well known to police.

Victor Calleja's car after the incident



67-year-old [John Camilleri](#), known as Giovanni tas-Sapun, died on 31 October 2016 when a bomb under his seat detonated at St Pauls bay. The bomb was

considered to be the most powerful one yet, and the car's roof ended up on a nearby penthouse. Camilleri owned S&S Bathrooms.





John Camilleri, 67, was killed by a car bomb in Bugibba

On 26 September 2016, 38-year-old man [Josef Cassar](#) was also targeted with a car explosive. Cassar, who was the sole director of S&T Services, lost both legs in the incident. The passenger was also injured. The bomb, which was reportedly full of screws and ball bearings, was placed under his car. The device was also believed to be detonated by a mobile phone.



Martin Cachia died in a car bomb in January 2016



CBRNE-TERRORISM NEWSLETTER – November 2017

On **23 March 2016**, a device detonated at a [boathouse](#) in Armier, which belonged to a 38-year-old man in Attard. No one was harmed in the incident.

On **16 January 2016**, [Martin Cachia](#), 56, was killed when a bomb detonated inside his car. It was not confirmed whether Cachia was the victim of the bomb, or if he was transporting it. Cachia was also known by the police, and was out on bail at the time of his death. He had pending court cases in connection with drugs, human trafficking and contraband cigarettes. He was also investigated in connection with smuggling fuel from Libya.

Back in **2015**, a bomb targeted a [Toyota showroom](#) in Haz-Zebbug on **6 July**. No one was injured during the attack, although damage was done to the showroom.

On **1 June 2014**, 35-year-old [Darren Degabriele](#) was killed when a bomb detonated underneath his car. The attack was also believed to have been triggered remotely. Degabriele owned a restaurant, as well as Degabriele fuels. He also operated a boat with frequent trips to Misurata, Libya.

On **3 November 2014**, a bomb detonated in front of police inspector [Geoffrey Azzopardi's home](#) in Zurrieq. The device was placed outside of the residence's garage door, which was blown off in the blast. No one was injured during the incident. At the time, Azzopardi was in charge of the Police EU funds unit at the Floriana headquarters and was formerly a CID officer.

Back in **September 2013**, an improvised explosive device was detonated in front of another boathouse in Armier. [Pierre Cremona and William Farrugia](#) noticed the device, which was attached to a mobile phone, and fled the area soon before the explosive went off. No one was hurt in this incident.



[Geoffrey Azzopardi's house was targeted in 2014](#)

Sources close to the investigation, said that the bomb was very similar to that placed under Paul Degabriele's pick-up truck.

In **2012**, Paul Degabriele's van was targeted with a parcel bomb. Degabriele had been alerted to the bomb and reported it to the police. The bomb contained three welded metal cylinders heavily packed with explosive

powders similar to fireworks. [Degabriele](#) would be shot dead a year later in Marsa.

Back in **November 2011**, a parcel bomb destroyed [Keith Galea's](#) car, three days after he was released from prison. Experts said that the bomb was likely detonated using a mobile phone, and was made with highly explosive material. No one was in the car at the time, and three people nearby were injured.



[The late Paul Degabriele and his wife, Anna Marie](#)

A month before, in **December 2010**, a bomb detonated outside [Transport Malta offices](#). The bomb was believed to have been intended for then head of the land transport section Konrad Pulé, who was injured in the explosion along with Peter Ripard.

Another five bomb attacks since 2010 targeted houses and a garage.

Pentagon Report: IED Casualties Surge in Afghanistan

Source: <http://foreignpolicy.com/2017/10/20/pentagon-report-ied-casualties-surge-in-afghanistan/>

Oct 20 – Improvised explosive devices have plagued the U.S. military and its allies since the earliest days of the fight against terrorism, leading the Pentagon at one point to declare a “Manhattan Project” to battle the homemade bombs. Now, 16 years later, the number of IED deaths and injuries is falling overall among countries under U.S. Central Command's authority, but not in Afghanistan.





The Afghan army conducts a controlled explosion during a military exercise on the outskirts of Kabul on April 30, 2014. (Shah Marai/AFP/Getty Images)

Some 3,043 people were killed or injured by IEDs in 1,143 incidents in Afghanistan between the beginning of April and the end of June of this year, according to internal slides from the Department of Defense obtained by Foreign Policy.

The numbers represent an 8 percent increase in incidents and a 39 percent increase in deaths and injuries compared to the previous 90 days. It's also a 17 percent increase the number of those killed or injured compared to the same period last year, even as the number of discrete incidents dropped 18 percent.

The report, produced by the Joint Improvised-Threat Defeat Organization (JIDO), the Pentagon's bomb-fighting agency, is marked for Official Use Only but based on open source reporting.

JIDO usually releases unclassified statistics two to three months after the events, a spokeswoman for the organization told FP in an email. She did not immediately respond to a request for those statistics.

Afghanistan was the only country in Central Command to see an increase in both incidents and casualties from IEDs compared to the previous 90 days, the JIDO report says. Iraq in the same period saw 15 percent fewer incidents and 30 percent fewer casualties than it had in the previous 90 days.

The question, of course, is why?

"In Afghanistan you have a stalemate that favors the insurgents," said Anthony Cordesman, an Afghanistan expert at the Center for Strategic and International Studies.

IEDs give insurgents "visibility, power, and influence," he said.

The Taliban may be turning to IED attacks because they can't control cities, Cordesman suggested. Whereas the Islamic State was able for a time to occupy cities in Iraq and Syria, the Taliban hasn't had the same success at home, and IEDs present a dramatic show of force with a terrible human cost. "IEDs, particularly attacks on civilian populations, get them immense visibility," he said.

IED attached to drone in Mexico could show evolution of drug cartel tactics

Source: <http://www.fox32chicago.com/news/national/ied-attached-to-drone-in-mexico-could-show-evolution-of-drug-cartel-tactics>

Oct 25 – The recent arrest in Mexico of four men carrying a drone equipped with an improvised explosive device "ready to be detonated" has stoked fears drug cartels could soon target the U.S. with bombs from above.

Mexican Federal Police arrested four men Oct. 20 in Guanajuato who were driving a stolen vehicle equipped with a 3DR Solo Quadcopter drone attached to an IED, Small Wars Journal reported. The drone had a range of about half a mile,



CBRNE-TERRORISM NEWSLETTER – November 2017

but modifications would have allowed it to fly farther.

State Attorney General Carlos Zamarripa Aguirre confirmed the arrests and the IED attached to the drone.

Aguirre said authorities investigated the drone, which contained a "significant amount of explosive and was ready to be detonated from a distance," AM reported.

"It is a drone," he said. "I have just confirmed that it is an explosive device, with a remote detonator and a large explosive charge."

The four men, identified as Christian N., Angel N., Eduardo N. and Marcos N. may be charged with terrorism, officials said. The men belonged to a "crime cell," but Aguirre refused to say which drug gang or cartel.

The area where the men were arrested was being contested by several cartels, including the Sinaloa, CJNG and Los Zetas. Since the beginning of 2017, organized crime has increased in the region.

Along with the drone and IED, authorities also said they found cellphones, an AK47, ammo and a remote detonator in the stolen vehicle.

Small Wars Journal reported the men appeared to fit the physical description of having been trained in the military or by law enforcement.

It was not immediately clear what type of IED was attached to the drone or what the target was.

Aguirre's office did not immediately respond to Fox News' request for comment.



WATCH | MORTAR SHELL, GRENADE, OR IED? Families returning to Marawi taught how to identify explosives

Source: <http://www.interaksyon.com/mortar-shell-grenade-or-ied-families-returning-to-marawi-taught-how-to-identify-bombs/>



Oct 24 – **Philippine teachers on Tuesday gave families returning to the destroyed lakeside city of Marawi a course on how to identify unexploded bombs in their homes and warned them to stay clear.**

The five-month battle to retake Marawi from pro-Islamic State rebels left the city in ruins. The government announced the end of military operations on Monday in the country's biggest security crisis in years, allowing rebuilding and rehabilitation efforts to begin..

The teachers taught children and their parents how to recognize live mortar shells, grenades, aircraft rockets and "improvised explosive devices" in their villages.

Security forces used artillery bombardment and air strikes to flush out the gunmen who endured 154 days of the offensive by stockpiling huge amounts of weapons, including bombs.



CBRNE-TERRORISM NEWSLETTER – November 2017

Warnings from the teachers included drawings of inquisitive children hammering bombs and trying to set them on fire.

"This helps us parents to understand and tell our children not to touch or get near the bombs," said Sobaida Sidic, a housewife attending the training.

Authorities said 920 militants, 165 troops and police and at least 45 civilians were killed in the conflict, which displaced more than 300,000 people.

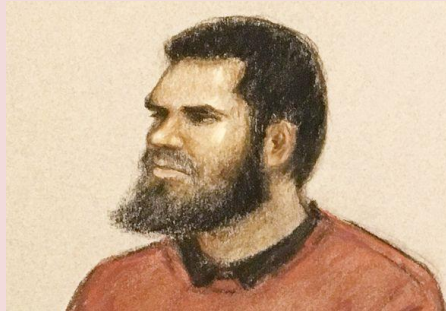
Lominog Manoga, a principal at a school in Marawi overseeing the training, said it was important to teach people the risks.

Philippine President Rodrigo Duterte had declared Marawi City liberated last week, even though fighting was not actually over. On Sunday, he said it was important to be vigilant because no country could escape Islamic State's "clutches of evil".

Suspected 'bomb maker' bought wrong type of nail varnish remover from Asda for 'terror attack explosives'

Source: <http://www.mirror.co.uk/news/uk-news/suspected-bomb-maker-bought-wrong-11454190>

Nov 02 – Asda CCTV footage shows a suspected 'bomb maker' buying the wrong type of nail varnish remover for '[terror attack](#)' explosives, a court has heard.



Sudanese immigrant Munir Mohammed allegedly enlisted the help of a chemist he met on a dating website in his plot to make explosives or deadly ricin poison.

Divorcees Mohammed and Rowaida El-Hassan allegedly had a "rapidly-formed emotional attachment and a shared ideology", despite living in Derby and London.

Mohammed also made contact with a so-called [Islamic State](#) commander and volunteered to carry out a terror attack in Britain, jurors at the Old Bailey, in London, heard.

The court was shown footage of the defendant visiting an

Asda store near his home on December 1 last year.

Prosecutor Anne Whyte QC told jurors when Mohammed was in the supermarket, he spoke on the phone to El-Hassan who sent him a link via WhatsApp to a website advertising a bottle of hydrogen peroxide, Ms Whyte also told the court his till receipt showed he had bought a bottle of Sally Hansen acetone-free nail polish remover.



[Munir Mohammed allegedly bought the wrong product on a trip to his local Asda \(Image: PA\)](#)

The prosecution say he saw the word "acetone" and assumed he was buying a component of TATP explosives, when in fact he had bought the wrong product.

On December 8, Mohammed visited Ace Discounts in Derby and looked at pressure cookers, which can be used to contain explosives, Ms Whyte had said.

On his arrest on December 12, police searched Mohammed's home and found two of the three components of TATP - hydrogen peroxide in a wardrobe, and a bottle of hydrochloric acid in the freezer, the court has heard.



CBRNE-TERRORISM NEWSLETTER – November 2017

An artists impression of Raiwada El-Hassan who is on trial for terror offences (Image: Julia Quenzler / SWNS.com)

El-Hassan had an unopened one-litre bottle of high percentage instant drain cleaner containing sulphuric acid, which can also be used to make explosives, as well as disposable face masks, jurors were told.

Mohammed told police he was going to clean his car alloys with the hydrochloric acid and had been advised by El-Hassan to use hydrogen peroxide to treat a burn.

Mohammed, 36, of Leopold Street, Derby, and El-Hassan, 33, of Willesden Lane, north-west London, deny preparing terrorist acts between November 2015 and December 2016.

The trial continues.

EOD Truck

Source: http://www.tarideal.com/Solutions/EOD_%7Cfamp%7C_IED/EOD_TRUCK/ED-TA01006/EOD_TRUCK



Rapidly deploys an EOD team, complete with all the required mission equipment. May be equipped with conventional bomb disposal equipment, disruptors, bomb suits, x-ray inspection equipment, searching devices, hazardous material response equipment, demolition tools, mine detectors, bomb locators, bomb container, various cartridges and various other specialized EOD tools according to customers requirements.

White Supremacists Share Bomb-Making Materials in Online Chats

Source: <http://counteriedreport.com/white-supremacists-share-bomb-making-materials-in-online-chats/>

Nov 02 – Right-wing extremists communicating in confidential online chats in recent months have shared scores of documents detailing the manufacture and use of bombs, grenades, mines and other incendiary devices.

The documents, which range from instructions on detonating dynamite to U.S. military manuals for constructing improvised explosives and booby traps, were passed around during online conversations among members of Anticom, a secretive and militant group that has emerged during the past year.



CBRNE-TERRORISM NEWSLETTER – November 2017

Records of the [online chats](#) were made available to ProPublica by Unicorn Riot, a leftist media collective that has reported critically on racist marches and right-wing political rallies in cities around the U.S.

Anticom, or Anti-Communist Action, views itself as a guerilla army fighting against what it has called the radical elements of the country's political left. On its social media channels, Anticom openly embraces fascist ideology and imagery, and the group's members have engaged in hate-filled talk involving Jews,

Muslims, immigrants and African Americans. In recent weeks Anticom has stepped out of the shadows as its members have provided security to so-called alt-right champion Richard Spencer at a speaking event in Florida. Anticom also helped to organize a "White Lives Matter" protest in Shelbyville, Tennessee, last weekend.

It is unclear how seriously the documents shared in the chats were explored by any of Anticom's members or followers, much less whether the documents were actually used to craft incendiary devices. But the transcripts of the chats include racist talk and open mentions of mass killings.

The user who posted the bomb-making documents, for instance, said he or she wanted

to overthrow the U.S. government. "Death to all non whites," the user wrote in a chat forum post on April 26. Another Anticom member encouraged recruits to construct a bomb and use it to carry out an attack in the style of the 2013 Boston Marathon bombing.

The chatroom logs shared with ProPublica show that Anticom members were in communication with another extremist group, several members of which have surfaced in federal investigations.

In May, federal agents searching the Tampa home of 21-year-old Brandon Russell discovered an array of explosives and bomb ingredients: fuses made from rifle shells, a white cake-like explosive substance called HMTD, more than one pound of ammonium nitrate and other explosive precursors, and two different kinds of radioactive material. The agents promptly arrested Russell, who was both a member of the Florida National Guard and a leader of Atomwaffen, a small fascist group calling for a "white revolution in the 21st century."

Federal authorities only uncovered Russell's bomb-making materials after his roommate and fellow Atomwaffen member Devon Arthurs killed two of their comrades. Arthurs later told law enforcement that he acted in order to prevent acts of domestic terrorism, and that Atomwaffen intended "to build a Fourth Reich." Russell participated in "neo-Nazi internet chat rooms where he threatened to kill people and bomb infrastructure," and was plotting to blow up a nuclear power plant near Miami, according to Arthurs.

After pleading guilty in September to illegally possessing explosive material and an unregistered destructive device, Russell is currently awaiting sentencing, which is scheduled for early next year.

Russell's attorney, Ian Goldstein, cast doubt on any link between Anticom and his client's explosives charges. Law enforcement didn't find any manuals for building bombs in Russell's home or on his computer, Goldstein said, adding Anticom and its online chats never came up during his research for the case.

Federal prosecutors in Florida would not comment on the case, or any potential overlap between Anticom and Russell and his neo-Nazi cell.

ProPublica asked the FBI whether it was looking into Anticom and the bomb plans. "The FBI does not confirm or deny specific investigations. However, any information regarding violent criminal activity or threats of terrorism should be reported promptly to the FBI," said a national FBI spokesperson.

Speaking broadly, the FBI representative noted that the bureau concerns itself with potential acts of terrorism, not unpopular political beliefs. "Our focus is not on membership in particular groups but on individuals who commit violence and other criminal acts. Furthermore, the FBI does not and will not police ideology."



CBRNE-TERRORISM NEWSLETTER – November 2017

Anticom, through a designated spokesperson, did not dispute the authenticity of the logs, but said the group had months ago taken steps to ban people threatening violence from the online chats.

"Of course we denounce that kind of behavior," the person said. "If an Anticom member built a bomb, he'd be banned as soon as we found out." Despite the intensely hateful views expressed by many Anticom members, the spokesperson said "all races and ideologies are welcome" in the organization so long as they "are anti-communist."

The person dismissed any suggestion that Anticom had a connection with Atomwaffen.

Anticom's size is unknown, but it boasts chapters in at least 15 U.S. and Canadian cities, and members have shown up waving the black-and-yellow Anticom flag at events across the country. (One of the organization's logos shows a person being hurled from a helicopter, a tactic used by right-wing death squads in Chile and Argentina.) Anticom's confidential online chats, which were conducted on an encrypted server hosted by service called Discord, give some sense of the organization's possible scale: people using more than 1,200 different usernames participated in the discussions.

Peter Simi, director of the Earl Babbie Research Center at Chapman University, noted that violent and radical talk are part of the culture of white extremist groups — and that talk typically does not lead to action. Still, he said the material was worrisome.

"All it takes is one person to do something with that information," said Simi, who has interviewed dozens of white supremacists and co-authored the book "American Swastika."

Over the span of about seven months this year — from early February to late September — Anticom members posted more than 90,000 messages on the Discord server before being kicked off the service by company officials. The online discussions include plenty of profanity-laden racist and anti-Semitic banter by people with usernames like "Augusto Pinochet," "deplorablepatriot," and "Hauptstürmführer Pepe." More worrisome, though, are the incitements towards violence.

On April 26, one Anticom member posed a question to the rest of the group: "Anyone want access to my pdf library?" the person wrote. "137 pdfs of how to manufacture explosives."

Saved in the PDF format, the cache of documents includes recipes for making potent bombs from ammonium nitrate, scientific papers on the chemical composition of different explosive agents, an Army manual on deploying anti-personnel mines, and a guide to using radio frequencies to detonate explosives, a tactic frequently used by insurgents in Iraq and Afghanistan.

Some of the bomb documents are highly technical, likely to be of little use to anyone but a skilled chemist or engineer. Other documents are old, like a 1984 book showing how to build hand grenades. As a whole, however, the documents could easily provide a person with the tools to kill and wound scores of people.

J.M. Berger, a fellow with the International Centre for Counter-Terrorism in the Netherlands, said social media companies like Discord tend to downplay the dangers posed by racial extremists using their networks and are often slow to curb their activities. "White supremacists and antigovernment extremists have always collected and distributed this kind of content. The internet makes that process easier and cheaper and more anonymous."

Berger said Discord should consider contacting law enforcement, if only out of a sense of caution. "It's probably not appropriate to freak out," Berger said, "but a situation like this merits more scrutiny."

A spokesperson for Discord, which is primarily used by video game enthusiasts who want to communicate by voice or text, while playing games, said the Anticom chats were shut down in September once Discord was "alerted to activity in violation of our terms of service." The company barred other white extremist groups off its servers in the aftermath of the lethal Unite the Right rally in Charlottesville in August. According to the spokesperson, Discord had not been in contact with any authorities, but would cooperate in any investigation should one be undertaken.

One Army manual shared by Anticom members offers step-by-step plans for creating fire bombs by adding chemicals to gasoline or other readily available fuels. But the documents go well beyond explosives. There are instructions on using military-type assault rifles and M249 machine guns, as well as hand-to-hand fighting techniques.

The chat logs also describe plans for engaging in violence at political events during the past year. In the days before an April 15 rally in support of President Donald Trump in Berkeley, California, one Anticom member promised the event would turn into a "bloodbath." After the rally, which was marked by a series of brutal street battles between right-wingers and leftists, another Anticom member boasted of breaking a rival's jaw in the fighting.



How Science Helped Detect The Powerful Explosive TATP In Unidentified Objects

Source: <http://counteriedreport.com/how-science-helped-detect-the-powerful-explosive-tatp-in-unidentified-objects/>



Nov 01 – Triacetone triperoxide (TATP) is a powerful explosive without military use because it is very sensitive to mechanical shock and so very difficult to safely handling, a reason for which terrorists dubbed TATP “the Mother of Satan”.

TATP is easily prepared from acetone and hydrogen peroxide under acidic catalysis, being a home-made explosive almost undetectable by dogs or sniffer devices usually trained for nitrogen-containing explosives. The possibility of being prepared on board gave rise to restrictions on carrying liquids in hand luggage at airports, and the careful monitoring of luggage and people, so TATP is presently one of the substances with more impact in the everyday life of millions of people who probably never heard about its existence. TATP is frequently used in suicide terrorist attacks, therefore constitutes a threat in public transport or mass events where prevention of indiscriminate attacks with explosives is a major concern. Manufacturers of explosive detectors tend to concentrate on X-rays for bulk materials, but the signature of TATP is not clearly visible except by bulky mass spectrometers. A consequence of this is that better systems still need to be developed. Looking for much simpler technologies, optical portable methods have been developed on the basis of colorimetric or fluorimetric sensor arrays for detection of TATP vapor, by detecting hydrogen peroxide from TATP decomposition, because TATP itself did not react with the probes. So the search for fluorogenic probes that are specific for TATP is still an unresolved problem required for the easy and portable detection of peroxide explosives in checking of unknown materials at police controls.

The ideal probe should have a strongly fluorescent reporter and a quenching group easily oxidizable by a mild oxidizing reagent in the absence of any solvent. Perylenediimides (PDIs) are strongly fluorescent compounds of known stability under light and air, suitable for high-value dendrimeric materials in bioimaging and gene delivery applications, therefore they are appropriate candidates for the reporter unit. Our approach consisted of a modification of a fluorescent perylenediimide core with one electron donor aryl group by the classic carbon-carbon coupling chemistry.

From the study of its physicochemical characteristics, its sensitivity to oxidants and its covalent anchoring to a polymer we have developed a fluorogenic material that was able to generate fluorescence in the presence of triacetone triperoxide, TATP, under solvent-free, solid-state conditions. The material, a perylenediimide functionalized polyacrylate, worked



by accumulating vapors of TATP, giving a colorimetric and strongly fluorescent response. The fluorescent response given by the material to the presence of TATP was permanent so it could be checked at any time after the TATP exposition. With the membrane, we developed an easy “white powder test” to detect solid TATP from suspect packages containing ‘white powder’ that could be involved in unidentified threats. In a typical experiment, a polymer piece from a vial with TATP acquired a strong orange fluorescence and pink color whilst an unreacted piece was non-fluorescent and purple colored, indicating the unequivocal presence of TATP in the white powder.

This study, [Solvent-Free Off-On Detection of the Improvised Explosive Triacetone Triperoxide \(TATP\) with Fluorogenic Materials](#) was recently published in the journal [Chemistry – A European Journal](#).

Reducing the Threat of Improvised Explosive Device Attacks by Restricting Access to Explosive Precursor Chemicals

Source: <https://www.nap.edu/read/24862/chapter/1#xii>

Improvised explosive devices (IEDs) are a type of unconventional explosive weapon that can be deployed in a variety of ways, and can cause loss of life, injury, and property damage in both military and civilian environments. Terrorists, violent extremists, and criminals often choose IEDs because the ingredients, components, and instructions required to make IEDs are highly accessible. In many cases, precursor chemicals enable this criminal use of IEDs because they are used in the manufacture of homemade explosives (HMEs), which are often used as a component of IEDs.

Many precursor chemicals are frequently used in industrial manufacturing and may be available as commercial products for personal use. Guides for making HMEs and instructions for constructing IEDs are widely available and can be easily found on the internet. Other countries restrict access to precursor chemicals in an effort to reduce the opportunity for HMEs to be used in IEDs. Although IED attacks have been less frequent in the United States than in other countries, IEDs remain a persistent domestic threat. Restricting access to precursor chemicals might contribute to reducing the threat of IED attacks and in turn prevent potentially devastating bombings, save lives, and reduce financial impacts.

Reducing the Threat of Improvised Explosive Device Attacks by Restricting Access to Explosive Precursor Chemicals prioritizes precursor chemicals that can be used to make HMEs and analyzes the movement of those chemicals through United States commercial supply chains and identifies potential vulnerabilities. This report examines current United States and international regulation of the chemicals, and compares the economic, security, and other tradeoffs among potential control strategies.





CYBER NEWS



DOD to remove Kaspersky software from Pentagon systems

Source: <http://www.homelandsecuritynewswire.com/dr20171024-dod-to-remove-kaspersky-software-from-pentagon-systems>

Oct 24 – The Department of Defense is reviewing its computer systems to make sure that software from under-suspicion Russian cybersecurity firm Kaspersky does not touch any military systems, a Defense spokeswoman [told](#) Nextgov.

In September DHS issued a [directive](#) to all civilian government agencies to remove Kaspersky software from their systems. The directive, which gave agencies three months to complete the removal, referred to deepening concerns in the U.S. intelligence community about the close relationship between Kaspersky and the Russian intelligence agencies.

The September directive did not apply to the Pentagon, which is outside DHS responsibility. Heather Babb, The Pentagon's spokeswoman said, though, that the Pentagon plans to "follow the intent of the directive" and that the DOD CIO is assessing what changes need to be made, if any.

Babb did not provide information on whether any military system is currently running Kaspersky software. NextGovnotes that in late 2014, DOD [funded](#) a contract for Kaspersky anti-virus software to be installed on 150 computers at the U.S. embassy in Cairo.

"The department actively reviews and ensures the security of its systems through a thorough screening process of all products to be used on the DOD information network," Babb said.

On Thursday, Assistant Secretary of Defense for Homeland Defense and Global Security Kenneth Rapuano told the Senate Armed Services Committee that officials "have instructed the removal of Kaspersky from all DOD information systems."

Intelligence officials have told NextGov said Kaspersky does not run on any of the systems of intelligence community, but that DOD has a much larger IT operation which is less self-contained.

The 13 September DHS directive does not say that the U.S. intelligence community found a direct link between Kaspersky and Russian intelligence, but only that the department is "concerned about the ties between certain Kaspersky officials and Russian intelligence" and about a Russian law requiring certain Russian companies to share source code with the government.

Company founder Eugene Kaspersky, a former KGB operative, has denied any ties between his company and Russian intelligence, but revelations about the extent of Russian interference in the 2016 U.S. election on behalf of Donald Trump has made the U.S. government more sensitive to the possibility of Russian cyberthreats.

On 5 October, the *Wall Street Journal* [reported](#) about a successful Russian hacking operation which leveraged Kaspersky anti-virus to steal National Security Agency hacking tools from an agency contractor's home computer. The *Journal* noted that it was not clear whether Kaspersky was aware of the Russian intelligence's use of the company systems, but cybersecurity experts said it is highly unlikely that the company could have been blind to the Russian intelligence's exploits.

NextGov notes that a military-wide ban on Kaspersky was included in the [Senate's version](#) of an annual defense policy bill which is now being negotiated between the House and Senate, and in separate [standalone legislation](#) introduced in June.

Is it time for a Cyber Peace Corps?

Source: <https://sciencenode.org/feature/is-it-time-for-a-cyber-peace-corps.php>

Oct 27 – Hackers around the world are attacking targets as diverse as [North Dakota's](#) state government, the [Ukrainian postal service](#) and a [hospital](#) in Jakarta, Indonesia. Unfortunately, many governments — in the developing world, and even cash-strapped [states and local communities](#) in the United States — lack the skills to effectively protect themselves.

The US has an opportunity to serve itself and the world by revitalizing the ideals of global service popularized in another era of its history. Congress should expand the mandates of the [Peace Corps](#) and [AmeriCorps](#) to create a Cyber Peace Corps. It could do this by amending the [Edward M. Kennedy Serve America Act](#), which was passed in 2009 to reorganize and expand the AmeriCorps program.



Expanding service options

Adding cybersecurity to the mandates of America's national and international service programs would help fight the dire [cyber-insecurity problems](#) facing the country and the world. The effort could bolster political support, and funding, for the Peace Corps and AmeriCorps. But more importantly, it could help train the [next generation](#) of cybersecurity professionals.

[Partnerships with universities](#) and community colleges across the nation could create summer cybersecurity boot camps and [clinics](#) to teach young Americans how to defend computer systems against malicious hackers. That would help address the [projected shortage](#) of 1.8 million cybersecurity professionals by 2022, and prepare prospective members of a [Cyber National Guard](#).

If Congress doesn't act, other options exist for both individuals and companies. A program like [Teach for America](#) could recruit willing volunteers and help prepare them for service. Private firms and civic groups could [create their own coalitions](#), perhaps along the lines of the [Service Corps of Retired Executives](#), linking trained professionals with communities needing help.

A similar effort in India, the nonprofit [Cyber Peace Foundation](#), has partnered cybersecurity experts with community organizations to help protect vulnerable populations, such as the [elderly](#).

Toward cyber peace

In the US, a pilot project could start with [existing industry organizations](#) focused on sharing cyber-threat information. Interested member corporations could contribute their workers for a fixed period of time to strengthen cybersecurity capabilities [in their communities](#), including for school districts, municipalities and utility companies. Firms with [international operations](#) could do the same abroad.

When President Kennedy called for the creation of the Peace Corps during the turbulent 1960 election, the world was different: At the height of the Cold War, America faced a difficult challenge to win [hearts and minds](#), especially in nations not yet aligned with either the US or the Soviet Union. Today [negative perceptions](#) about the United States are rising around the world.

Developing US cybersecurity talent and deploying it to mitigate [threats to information security](#) both at home and abroad would help protect vulnerable communities and rebuild social ties.

In fact, the efforts involved in getting Cyber Peace Corps workers and their hosts to work together to protect potentially sensitive information may help [strengthen trust](#) and goodwill among nations. And it would recast 20th-century service commitments to face 21st-century challenges.

There are untold thousands of people on college campuses, working for small businesses and in leading tech firms who are [worried about](#) the world's lack of cybersecurity, but who feel powerless to change things. If given an opportunity, their work would help create the next generation of cybersecurity professionals. And it could offer new opportunities to bridge partisan divides at home, and geopolitical fault lines abroad.

Bad Rabbit: New Ransomware Attack Rapidly Spreading Across Europe

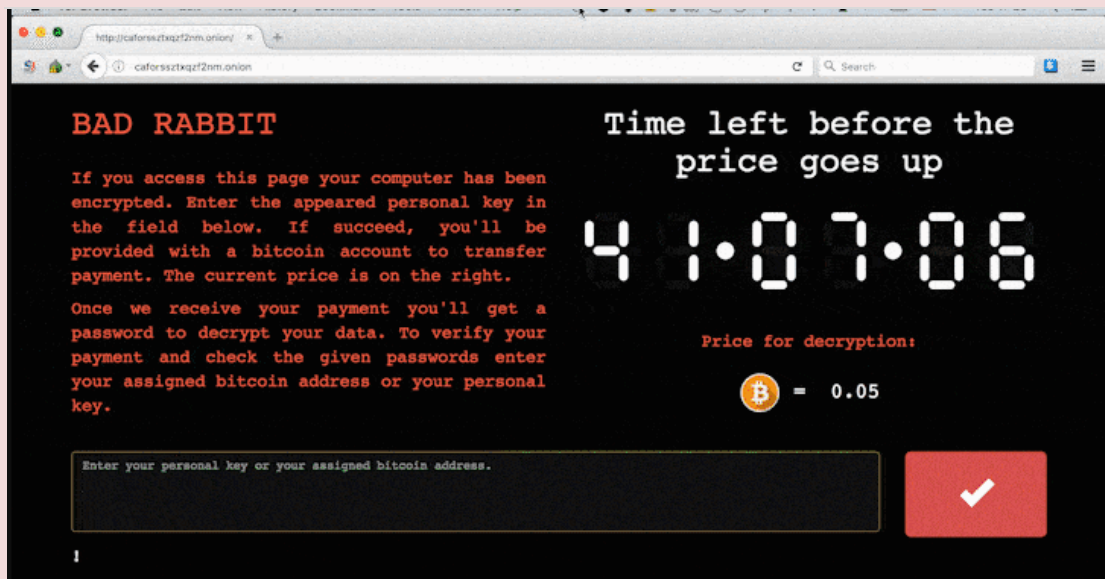
By Mohit Kumar

Source: <https://thehackernews.com/2017/10/bad-rabbit-ransomware-attack.html?m=1>

Oct 24 – A new widespread ransomware attack is spreading like wildfire around Europe and has already affected over 200 major organisations, primarily in Russia, Ukraine, Turkey and Germany, in the past few hours.

Dubbed "Bad Rabbit," is reportedly a new Petya-like targeted ransomware attack against corporate networks, demanding 0.05 bitcoin (~ \$285) as ransom from victims to unlock their systems.

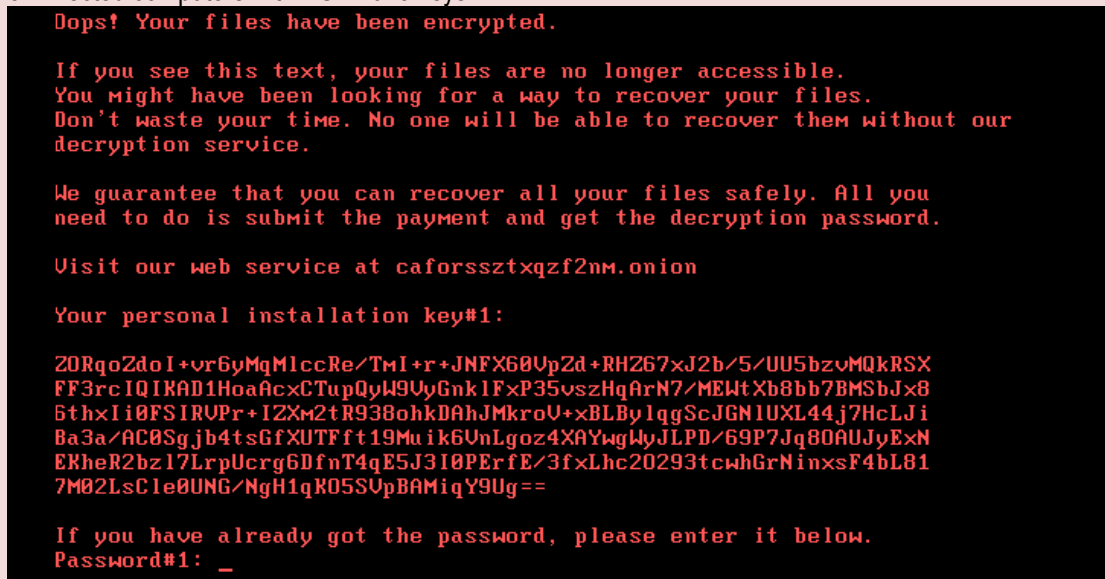




According to an initial analysis provided by the Kaspersky, the ransomware was distributed via drive-by download attacks, using fake Adobe Flash players installer to lure victims' in to install malware unwittingly. "No exploits were used, so the victim would have to manually execute the malware dropper, which pretends to be an Adobe Flash installer. We've detected a number of compromised websites, all of which were news or media websites." Kaspersky Lab [said](#).

However, security researchers at ESET have [detected](#) Bad Rabbit malware as 'Win32/Diskcoder.D' — a new variant of [Petya ransomware](#), also known as Petwrap, NotPetya, exPetr and GoldenEye.

Bad Rabbit ransomware uses DiskCryptor, an open source full drive encryption software, to encrypt files on infected computers with RSA 2048 keys.



ESET believes the new wave of ransomware attack is not using [EternalBlue exploit](#) — the leaked [SMB vulnerability](#) which was used by [WannaCry](#) and Petya ransomware to spread through networks.

Instead it first scans internal network for open SMB shares, tries a [hardcoded list](#) of commonly used credentials to drop malware, and also uses [Mimikatz](#) post-exploitation tool to extract credentials from the affected systems.

The ransom note, shown above, asks victims to log into a [Tor onion website](#) to make the payment, which displays a countdown of 40 hours before the price of decryption goes up.

The affected organisations include Russian news agencies [Interfax](#) and [Fontanka](#), payment systems on the Kiev Metro, Odessa International Airport and the Ministry of Infrastructure of Ukraine.



CBRNE-TERRORISM NEWSLETTER – November 2017

Researchers are still analyzing Bad Rabbit ransomware to check if there is a way to decrypt computers without paying ransomware and how to stop it from spreading further.

How to Protect Yourself from Ransomware Attacks?

Kaspersky suggest to disable *WMI service* to prevent the malware from spreading over your network. Most ransomware spread through phishing emails, malicious adverts on websites, and third-party apps and programs.

So, you should always exercise caution when opening uninvited documents sent over an email and clicking on links inside those documents unless verifying the source to safeguard against such ransomware infection.

Also, never download any app from third-party sources, and read reviews even before installing apps from official stores.

To always have a tight grip on your valuable data, keep a good backup routine in place that makes their copies to an external storage device that isn't always connected to your PC.

Make sure that you run a good and effective anti-virus security suite on your system, and keep it up-to-date.

Mohit Kumar is entrepreneur, hacker, speaker, founder and CEO — The Hacker News and The Hackers Conference

ISIS Hacks 800 School Websites Across the US

Source: <https://clarionproject.org/isis-hacks-800-school-websites-across-us/>



Nov 08 – Eight hundred school websites across the U.S. were [hacked by ISIS](#) on Monday, November 7. The hack lasted close to two hours, during which time visitors to the sites were redirected to a YouTube video with Arabic audio and pictures of Saddam Hussein. Text also appeared which read, "I love Islamic State (ISIS)."

The websites are all hosted by a company called School Desk (schooldesk.net) and are all connected to a server in Georgia.

School Desk has given a copy of the server to the FBI. Some schools have also hired outside security firms to help track down the hackers.

All the affected websites have been shut down to aid the FBI in its investigation.

"You always think it happens somewhere else, and now it's hitting home," said Nicole Tierney, who is connected to a school in New Jersey whose site was hacked.



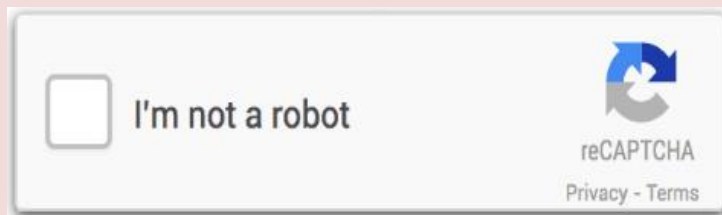
"It's upsetting to us," said Rob Frierson, the owner of School Desk, speaking to *CBS New York*. "We've been running this business for 17 years, and we've never had any sort of incident even remotely like this."

The challenge of authenticating real humans in a digital world

By Jungwoo Ryoo

Source: <http://www.homelandsecuritynewswire.com/dr20171108-the-challenge-of-authenticating-real-humans-in-a-digital-world>

Nov 08 – Proving identity is a routine part of modern daily life. Many people must show a driver's license to buy alcohol at a store, [flash an ID card](#) to security guards at work, enter passwords and passcodes to retrieve email and other private information, and answer security validation questions when calling banks or credit card companies for customer service.



Authentication is also [getting easier](#) for people: Take the iPhone, for example. Unlocking the early versions required a multi-digit passcode. Then Apple introduced [Touch ID](#), which would

unlock the phone with a fingerprint reader. The latest version, just out, is the [iPhone X](#), which can use its camera to perform [facial recognition](#) to [authenticate a user](#).

As a software security researcher looking at [authentication technologies for hand-held devices](#), I am fully aware that the technologies change, but the challenge remains the same: How can a digital system authenticate an analog human's identity?

Three factors of identity

There are [three main ways](#) of proving an identity. One involves something you know – like a password or your mother's maiden name. This method assumes the authorized user will have information no unauthorized user does. But that's not always the case: For [145.5 million Americans](#) affected by the [Equifax security breach](#) revealed in September 2017, reams of previously private information may now be known to criminals.

A second method of authentication is with something you have – such as a key to your home's front door or a smart card to swipe at work. This assumes a limited number of people – possibly as few as one, but it could be a small group of users, like a family or co-workers – are allowed to enter a physical space or use a digital service.

A third way is by authenticating the individual human being – who you are – with some aspect of your biology. There are various type of these biometrics, such as fingerprints, [facial recognition](#), iris scanning and [voiceprints](#). This strategy, of course, assumes that the bodily feature is unique to the particular individual – and, crucially, that the digital system involved can tell the difference between people.

Using two or more methods together can improve security and is called [two-factor, or multi-factor, authentication](#).

The consequences of digital authentication

This increasing dependence on digital authentication may actually result in less security. While cameras, sensors and other devices can make authentication easier for people to accomplish, they carry their own weaknesses.

When a system seeks to authenticate an individual, it must compare the [information the person is presenting](#) – what they know, what they have or who they are – against a previously stored database of authorized users. As the [Equifax security breach](#) makes clear, those databases are themselves vulnerable to attack. Information stolen from there could be used somewhere else – for instance, to identify which bank a particular person uses and answer security questions when calling to transfer money. Or the database itself could be corrupted, altering information so an attacker would be able to fake his way into a physical space or system.

Another potential security threat inherent in biometrics in particular is that criminals don't need to



CBRNE-TERRORISM NEWSLETTER – November 2017

guess a password, or force someone to reveal it: The simple presence of the victim – even at gunpoint – can supply the fingerprint or face to authenticate and unlock a system.

Future complications

As authentication becomes more complicated, using multiple factors and secure communications between sensors and databases, [users become less willing](#) to jump through all the hoops. So security managers try to make the process easier for them without weakening the protections. This commonly happens on websites that urge users to log in [using their Facebook or Google accounts](#); those sites rely on the advanced security of the tech giants rather than creating their own authentication systems.

In one futuristic scenario, authentication could occur without a user even noticing: When you

walk into a store, facial recognition could identify and authenticate you. Then, at checkout, you'd need only to scan your purchases and leave – the store will automatically charge the credit card of your choice. This isn't science fiction: Amazon has [patented a system](#) for doing exactly this in its [Amazon Go cashier-less convenience stores](#).

This is possible in part because of the increasingly common practice of [computer systems authenticating each other](#) – so the store's system would recognize you, connect to the credit card company and authorize your purchase all on its own.

It may be more convenient, and even more secure, than a magnetic strip on a plastic card in your wallet. But the potential dangers will require much higher security for private information, particularly [biometric data](#). A real identity still comes down to flesh and blood.

Jungwoo Ryoo is Professor of Information Sciences and Technology at Altoona campus, Pennsylvania State University.

Cryptoterrorism: Do Cryptocurrencies Facilitate Terrorism?

Source: <https://themarketmogul.com/cryptoterrorism-far-cryptocurrencies-come-financing-terror/>



Nov 12 – The terrorists of today are innovators – they evolve tactics to adapt to the constant intelligence forces across the world. One such example exists in the increasingly prevalent yet volatile world of cryptocurrencies. The use of cryptocurrencies to fund terror groups has gained traction recently.

Islamic Extremism

In June 2016, the Ibn Tamiya Media Centre (ITMC), which serves as the online propaganda arm of the Salafi jihadist group Mujahedeen Shura Council (designated as a terrorist group by the US State Department), added the option of donating in bitcoin on its 'Jahezona' ('equip us') campaign. This was done in the form of QR codes posted onto [Twitter](#). In early 2017, operatives from the Islamic State were found to have used bitcoin and [PayPal](#) in sending funds to local Islamists in Indonesia, according to the PPTAK, an independent anti-money laundering agency.

This has led to a series of nationwide crackdowns on bitcoin's potential for abuse by a number of countries. In August 2017, Australia began regulating digital currency exchanges.



CBRNE-TERRORISM NEWSLETTER – November 2017

Reforms aimed at strengthening the Anti-Money Laundering and Counter Terrorism Financing Act have resulted in cryptocurrency providers such as bitcoin being brought under the remit of the Australian Transactions and Reporting Analysis Centre (ATRAC). This follows similar regulatory attempts on cryptocurrencies in China, wherein the People's Bank of China threatened several exchanges with closure in the event of violations of existing anti-laundering regulations.

On the surface, the anonymity attached to cryptocurrencies would implicate rampant use among terrorist organizations and their donors. Their use, however, has not been widespread thus far. In the aforementioned case, the inclusion of bitcoin has led to just over \$500 worth of digital currency being channelled towards [Jahezona](#).

The Scale of the Problem

This non-prevalence is due to several factors, including how bitcoin, in particular, is fast becoming mainstream. Sarah Meiklejohn, a computer scientist at University College London, describes how from the point of view of investigators, blockchain serves as a ready-made criminal history record, referring to the [Silk Road](#) bust of 2015. This limitation of anonymity is reflected further the limitation in the acceptance of cryptocurrencies in the areas where terrorist group largely operate. This puts a greater dent in their appeal as a source of finance.

Moreover, the current financing models neither accommodate nor necessitate, cryptocurrency funding. Radicalized 'lone wolf' attackers are largely self-financed, with foreign fighters raising capital to travel to their intended destinations via crowdfunding platforms such as Kickstarter. The majority of terrorist organizations in the Middle East, on the other hand, rely on the pre-existing (not to mention dominant) 'hawala' network of transfers, in which anonymous payments and donations to terrorist groups are made through brokers.

In stating this, however, room for evolution cannot be dismissed. Already improvements are being made towards preserving and enhancing anonymity for cryptocurrencies. 'Dark Wallets' have emerged in recent years. Made by companies such as the eponymous Dark Wallet and BitcoinFog, they allow not only greater anonymity but render transactions almost untraceable. In a 2014 article, Dark Wallet co-founder Cody Wilson speaks of how he, "wanted a private means for black market transactions, whether they were for non-prescribed medical inhalers, MDMA for drug enthusiasts, or weapons". Additionally, cryptocurrencies such as [Zcash](#) allows for secure offline transaction and storage of assets, providing greater barriers for regulators.

Next Steps

The Islamic State, the once powerful aspirant caliphate that bulldozed through swathes of territory across Iraq and Syria, is now in retreat – but far from defeated. As many analysts have pointed out, their mode of operations would most likely switch from the head-on confrontation with forces back to the traditional guerrilla warfare mode. As they would change their mode of conflict, so would they seek ways to finance their operations. Anonymous and untraceable means to do so, of which cryptocurrencies are becoming better suited towards doing, provide more than attractive options for funding.

To conclude, while cryptocurrencies' impact in terrorist funding is not significant as of now, the landscape, given current developments, promises to change. Hence, governments should adopt prudent measures tackling cryptocurrency abuse, whilst simultaneously ensuring that this technology is protected and not vilified. Thus, it is imperative for governments and providers to form or at the very least deliberate initiatives ensuring the most important protection of all-that of the lives of innocent citizens.

NATO launches Cyber Operations Center

Source: <http://www.homelandsecuritynewswire.com/dr20171110-nato-launches-cyber-operations-center>

Nov 10 – Russia's successful cyber-interference on behalf of its favored candidates, parties, and causes in the United States, France, the Netherlands, Germany, and the United Kingdom; its effective cyberattacks on infrastructure facilities in Ukraine and the Baltic states; and the

growing cyberthreats from China, North Korea, and Iran, have convinced the member states of NATO that these threats must be met in a more systematic and comprehensive fashion.



CBRNE-TERRORISM NEWSLETTER – November 2017

The defense ministers of NATO members states, in a meeting earlier this week, endorsed a set of principles for how the Alliance can integrate the cyber capabilities of its Allies into Alliance military operations. Ministers also agreed to the creation of a new Cyber Operations Center to help integrate cyber into NATO planning and operations at all levels. This follows steps last year to recognize cyber as an operational domain along with land, sea and air. NATO Secretary General Jens Stoltenberg, after outlining different initiatives launched at the meeting of the North Atlantic Council earlier this week, said:

Finally, we discussed ways to strengthen our cyber defenses. We must be just as effective in the cyber domain as we are on land, at sea and in the air, with real-time understanding of the threats we face and the ability to respond however and whenever we choose. Today, ministers agreed on the creation of a new Cyber Operations Centre as part of the outline design for the adapted NATO Command Structure. This will strengthen our cyber defenses, and help integrate cyber into NATO planning and operations at all levels. We also agreed that we will be able to integrate Allies' national cyber capabilities into NATO missions and operations. While nations maintain full ownership of those

capabilities. Just as Allies own the tanks, the ships and aircraft in NATO missions.

Franklin D. Kramer, a distinguished fellow in the Atlantic Council's Brent Scowcroft Center on International Security and an Atlantic Council board member, said NATO's cyber initiative is a big deal.

The Alliance has "always had significant conventional capabilities—land, air, and sea—now cyber can be included," Kramer [told the New Atlanticist](#). "The value of the cyber operations center is that it will integrate the cyber capabilities with all of the rest of NATO's military capabilities," he said.

There is uncertainty surrounding the level of offensive cyber-capabilities and how they may be implemented, but the new cyber command will facilitate NATO's responses to cyberattacks, which, as of the 2016 Warsaw Summit, could elicit an Article 5-level response. Article 5 of the NATO charter stipulates that if one ally is attacked, all members of the Alliance will come to its defense (see "EU set to define cyberattacks as 'acts of war,' allowing collective military response," [HSNW, 30 October 2017](#)).

"The decisions with respect to the cyber center simply allows NATO to respond more effectively [to an attack] if necessary, because there is a structure for it," said Kramer. Ultimately, he said, the operations center will facilitate a proportionate reaction to a threat, by either conventional or cyber means.

Biology can show us how to stop hackers

Source: <http://www.homelandsecuritynewswire.com/dr20171110-biology-can-show-us-how-to-stop-hackers>

Nov 10 – [Stephanie Forrest](#) is the director of the [ASU Biodesign Institute](#) Center for Biocomputing, Security and Society, and she is a professor in the [School of Computing, Informatics and Decision Systems Engineering](#). She has more than twenty years of experience leading interdisciplinary research and education programs, particularly at the intersection of biology and computation, including work on computer security, software engineering and biological modeling.

ASU Now [spoke](#) with Forrest about her take on the computer security landscape and what computer scientists can learn from human immune systems and biological evolution.

ASU Now: You research the intersection of biology and computation. What can biology teach us about computer security?

Stephanie Forrest: Biology is the true science of security. And by that I mean that organisms have had to contend with adversaries and competitors from the very beginning of their evolutionary history. As a result, they've evolved an incredible repertoire of defense systems to protect themselves. Every cell has a defense system, and every kind of animal has a defense system, and even ecological systems have defenses built-in.

Looking at how biological systems have learned to protect themselves can suggest novel approaches to security problems. One of the easiest places to see this is in the immune system, which plays a major role in protecting individual organisms from foreign viruses and bacteria. What I try to do is look at biological



mechanisms and principles and translate those mechanisms and architectures into computational algorithms that protect computers.

AN: *What is your take on the scope of data breaches over the past decade?*

Forrest: We consumers don't have as deep an understanding of the scope of these breaches as we should. Today, we're essentially forced, either through our jobs or just to conduct our lives, to give up huge amounts of personal information to third parties, who have demonstrated time and again that they cannot protect it. As a result, our data are everywhere — in the hands of foreign governments, in the hands of cybercriminals, in the hands of the media, and in the hands of corporations we may never have heard of.

The impact of leaked data is just as important as the number of stolen records. We know that data about millions of people has been taken. But if you are never actually hurt by the stolen information, as in, you've never had money stolen or been blackmailed, are you harmed just by people knowing your credit score?

Courts have ruled on this, and in my view, they have set what is an unobtainable standard: you have to prove that you have been harmed. So if my personal information is in a database that gets hacked, unless the criminal uses it to do something like steal my money, and unless I can prove that that specific criminal used that specific data to steal my money, I can't sue the person responsible for the database that was breached.

That seems like an impossible standard. If there are several copies of my social security number out in the world, how can I prove which copy was the one that let the criminal take my money?

AN: *Why are current computer systems so vulnerable to hacking?*

Forrest: Part of the problem is how the tech industry has grown up, and it's very difficult technically to go back and retrofit systems to prevent problems we're seeing today. Our IT systems today consist of many tightly integrated systems of software that talk to each other, and they're all controlled by different organizations, companies and institutions.

When something bad happens, even if you could assign fault, that fault is usually distributed over so many entities that there's no effective stick. The carrot is for companies to make more money producing more technology in our lives and increasing our dependence on it. There's

nothing reigning that back. We also don't have software liability or consumer protection, even though software is widely used by everyone.

Another issue is that cloud storage and cloud computing have exacerbated our vulnerability. In the old days, my data were just on my own computer, and if my own computer got hacked, it was just my information that was lost. Now that my data are merged with everyone else's, like with Equifax, then one breach has enormous impact.

AN: *What are the biggest security challenges we'll face in the near future?*

Forrest: The immediate challenge is the internet of things. In addition to the insecure software and networks we already have, we're adding devices that interact with our physical lives. We're already doing a poor job of securing our software systems, but once these systems have the ability to control our physical and virtual environments, the complexity and risks go up dramatically.

Another risk I see is the possible end to the general purpose computer. As a computer scientist, this terrifies me. The flexibility of computing and software produced the wonderful technology we have today. Today's computing devices are incredibly general and because of that, they can do a wide range of things. I worry that, in the rush to secure our systems, the easiest path will be to restrain functionality. Losing that general purpose computing ability would be a terrible loss, not just for computer scientists, but also for society.

We also have real questions about how the growth of technology and its securities or insecurities will interact with our democratic process. We in the U.S. value free speech more than any other place in the world. But, I think we're seeing the limits of that and we need to reformulate what free speech means in the context of a world with social media platforms. Having some kind of public discourse about this is important, and it will have an impact on cybersecurity.

Another future challenge will be in the area of consumer protection. My concern here is that we should be having the public discourse now about what the principles are that we as a society want to embrace, rather than just waiting for another crisis and a knee-jerk reaction. I fear something serious happening, say a massive cyber-enabled power failure or manipulation of the financial



markets, and suddenly there is pressure to pass a law gets passed requiring, e.g., that any device with access to the internet has to run a particular type of software. That would be

counterproductive, and against our principles, but it also would increase our overall risk because it would create new single points of failure.



Boeing 757 hacked on the tarmac by Department of Homeland Security in 'controlled experiment'

Source: <https://www.computing.co.uk/ctg/news/3020901/dhs-team-manages-to-hack-boeing-757>



Nov 13 – A team of aerospace experts working with the US Department of Homeland Security to conduct a controlled hacking of a Boeing 757 on the ground at an Airport in Atlantic City, New Jersey.

The team of academics and industry experts were able to remotely crack the IT systems of the 757, which uses a form of computerised fly-by-wire system for control. The test demonstrates the inadequacy of security in many modern plans that, nevertheless, rely on IT to stay airborne.

The controlled experiment led by the Department of Homeland Security was conducted in September 2016, with the pilots unaware of the experiment taking place.

The researchers exploited the plane's own wireless communications to penetrate its internal network. Robert Hickey, aviation program manager working at the company's Cyber Security Division, detailed the experiment during a keynote speech at the CyberSat Summit 2017.

He said that the researchers only needed two days to develop and execute a hacking strategy, but they relied on a "classified" pool of resources.

Aviation and IT security experts were, apparently, aware of the security flaws discovered by DHS. However, pilots working for normal airline companies weren't briefed until March 2017.

[According to aviation news site Aviation Today](#), Hickey said: "All seven of them broke their jaw hitting the table when they said.

"You guys have known about this for years and haven't bothered to let us know because we depend on this stuff to be absolutely the bible."

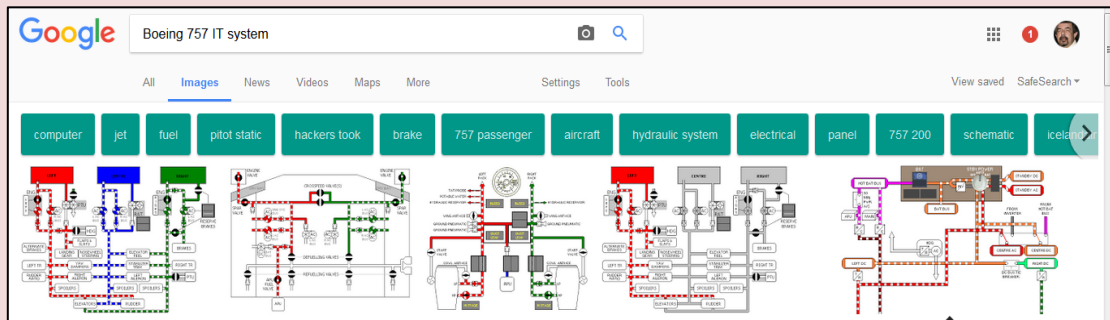
Despite the fact that mass production of the 757 ended in 2014, it's still used by companies across the world. Around 90 per cent of commercial planes consist of such legacy models, although not all utilise fly-by-wire avionics.

However, the cost of amending computer systems on board aircraft might hamper efforts at improving security. According to Aviation Today, it can cost \$1m and take a year to change just one line of code in one aircraft.

While older models, like the 757, might lack appropriate security, more modern and current production models ought to be more secure, added Hickey.



EDITOR'S COMMENT: I was looking for a photo of Boeing's IT system at Google Images and I found all the basic details of its hydraulics, fuel system, pneumatics, electrics and much more – some



were animated as well. And the article reads about hacking, the moment everything is on line...



Amazon and Toys R Us urged to withdraw toys that allow hackers to exploit Bluetooth flaw to talk to children

Source: <http://www.scmp.com/news/world/article/2119790/amazon-and-toys-r-us-urged-withdraw-toys-allow-hackers-exploit-bluetooth>

Nov 15 – A consumer group is urging major retailers to withdraw a number of “connected” or “intelligent” toys likely to be popular at Christmas, after finding security failures that it warns could put children’s safety at risk.

Tests carried out by Which? with the German consumer group Stiftung Warentest, and other security research experts, found flaws in Bluetooth and Wi-fi-enabled toys that could enable a stranger to talk to a child.

The investigation found that four out of seven of the tested toys could be used to communicate with the children playing with them. Security failures were discovered in the Furby Connect, i-Que Intelligent Robot, Toy-Fi Teddy and CloudPets.

With each of these toys, the Bluetooth connection had



not been secured, meaning the researcher did not need a password, pin or any other authentication to gain access. Little technical know-how was needed to hack into the toys to start sharing messages with a child.

When switched on, the Furby Connect – on sale at Argos, Amazon, Smyths and Toys R Us – could be connected with any device within a Bluetooth range of 10 to 30 metres.

With the i-Que Intelligent Robot, the investigation discovered that anyone could download the app, find an i-Que within their Bluetooth range and start using the robot’s voice by typing into a text field. The toy is made by Genesis, which also

manufactures the My Friend Cayla doll, recently banned in Germany owing to security and hacking concerns.

CloudPets toys, on sale at Amazon, are stuffed animals that enable friends to send a child messages that are played on a built-in speaker. But Which? found the toy could be hacked via its unsecured Bluetooth connection.



CBRNE-TERRORISM NEWSLETTER – November 2017

Also available from Amazon, the Toy-Fi Teddy allows a child to send and receive recorded messages over Bluetooth via a smartphone or tablet app. Which? found the Bluetooth connection lacked any authentication protections, meaning hackers could send voice messages to a child and receive answers. “Connected toys are becoming increasingly popular, but as our investigation shows, anyone considering buying one should apply a level of caution,” said Alex Neill, the managing director of home products and services at Which?.

“Safety and security should be the absolute priority with any toy. If that can’t be guaranteed, then the products should not be sold.”

Which? has written to retailers to urge them to stop selling connected toys that have proven security issues.

Argos said in a statement: “The safety of the products we sell is extremely important to us. We haven’t received any complaints about these products but we are in close contact with the manufacturers, who are already looking into [these] recommendations.”

Hasbro, which makes the Furby Connect, said: “Children’s privacy is a top priority, and that is why we carefully designed the Furby Connect and the Furby Connect World app to comply with children’s privacy laws. We feel confident in the way we have designed both the toy and the app to deliver a secure play experience.”

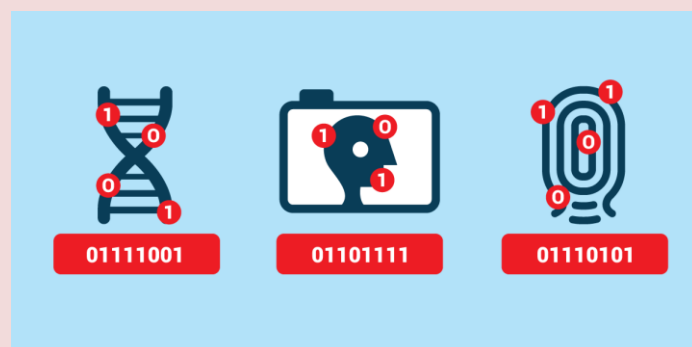
TSA Plans to Use Face Recognition to Track Americans Through Airports

Source: <https://www.eff.org/deeplinks/2017/11/tsa-plans-use-face-recognition-track-americans-through-airports>

Nov 09 – **The “PreCheck” program** is billed as a convenient service to allow U.S. travelers to “[speed through security](#)” at airports. However, the [latest proposal](#) released by the Transportation Security Administration (TSA) reveals the Department of Homeland Security’s greater underlying plan to collect face images and iris scans on a nationwide scale. DHS’s programs will become a massive violation of privacy that could serve as a gateway to the collection of biometric data to identify and track every traveler at every airport and border crossing in the country.

Currently TSA collects [fingerprints](#) as part of its application process for people who want to apply for PreCheck. So far, TSA hasn’t used those prints for anything besides the mandatory background check that’s part of the process. **But this summer**, TSA ran a [pilot](#)

[program](#) at Atlanta’s Hartsfield-Jackson Airport and at Denver International Airport that used those prints and a contactless fingerprint reader to verify the identity of PreCheck-approved travelers at security checkpoints at both airports. Now TSA wants to roll out this program to airports across the country and expand it to encompass face recognition, iris scans, and other biometrics as well.



From Pilot Program to National Policy

While this latest plan is limited to the more than 5-million Americans who have chosen to apply for PreCheck, it appears to be part of a broader push within the Department of Homeland Security (DHS) to expand its collection and use of biometrics throughout its sub-agencies. For example, in pilot programs in Georgia and Arizona last year, Customs and Border Protection (CBP) used face recognition to capture pictures of travelers boarding a



CBRNE-TERRORISM NEWSLETTER – November 2017

[flight out of the country](#) and [walking across a U.S. land border](#) and compared those pictures to previous recorded photos from passports, visas, and “other DHS encounters.” In the Privacy Impact Assessments (PIAs) for those pilot programs, CBP said that, although it would collect face recognition images of all travelers, it would delete any data associated with U.S. citizens. But what began as DHS’s biometric travel screening of foreign citizens [morphed, without congressional authorization](#), into screening of U.S. citizens, too. Now the agency plans to roll out the program to other border crossings, and it says it will retain photos of U.S. citizens and lawful permanent residents for two weeks and information about their travel for 15 years. It retains data on “non-immigrant aliens” for 75 years.

CBP has stated in [PIAs](#) that these biometric programs would be limited to international flights. However, over the summer, we [learned](#) CBP wants to vastly expand its program to cover domestic flights as well. It wants to create a “biometric” pathway that would use face recognition to track all travelers—including U.S. citizens—through airports from check-in, through security, into airport lounges, and onto flights. And it wants to partner with commercial airlines and airports to do just that.

Congress seems poised to provide both TSA and CBP with the statutory authority to support these plans. As we noted in earlier [blog posts](#), the “[Building America’s Trust](#)” Act would require the Department of Homeland Security (DHS) to collect biometric information from all people who exit the U.S., including U.S. and foreign citizens. And the [TSA Modernization Act](#), introduced earlier this fall, includes a provision that would allow the agencies to deploy “biometric technology at checkpoints, screening lanes, bag drop and

boarding areas, and other areas where such deployment would enhance security and facilitate passenger movement.” The Senate Commerce Committee approved the TSA bill in October.

DHS Data in the Hands of Third Parties

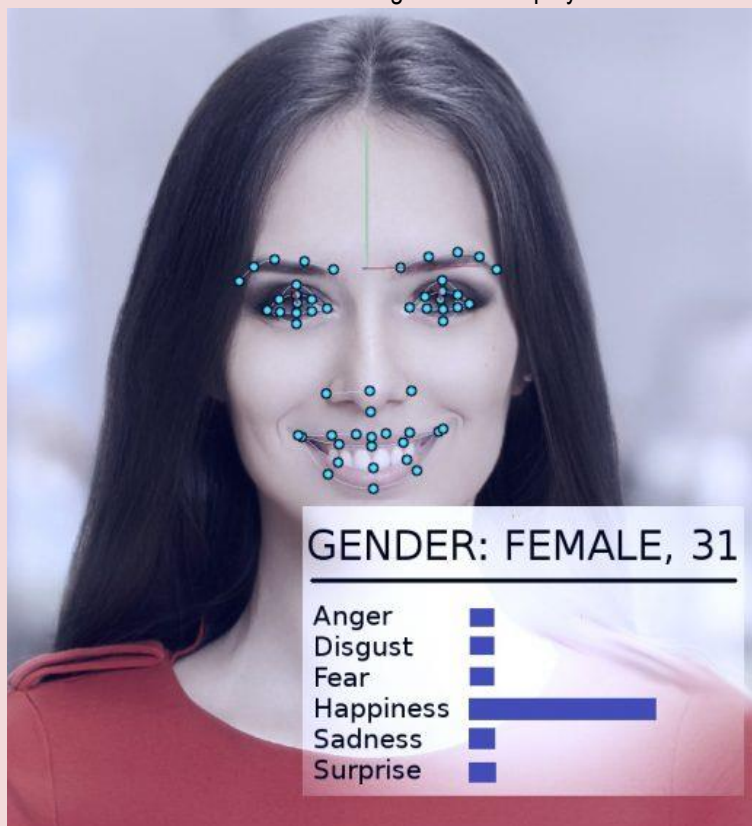
These agencies aren’t just collecting biometrics for their own use; they are also sharing them with other agencies like the FBI and with “private partners” to be used in ways that should concern travelers. For example, TSA’s PreCheck program has already expanded outside the airport context. The vendor for PreCheck, a company called Idemia (formerly MorphoTrust), now offers expedited entry for PreCheck-approved travelers at [concerts](#) and [stadiums](#) across the country. Idemia says it will equip stadiums with biometric-based technology, not just for security, but also “to assist in fan experience.” Adding face recognition would allow Idemia to track fans as they move throughout the stadium, just as another company, [NEC](#), is already doing at a professional soccer stadium in Medellin, Columbia and at an LPGA championship event in California earlier this year.

CBP is also exchanging our data with private

companies. As part of CBP’s “[Traveler Verification Service](#),” it will partner with commercial airlines and airport authorities to get access to the facial images of travelers that those non-government partners collect “as part of their business processes.” These partners can then access CBP’s system to verify travelers as part of the airplane boarding process, potentially doing away with boarding passes altogether. As we saw earlier this year, several airlines are already planning to implement their [own face recognition](#) services to [check bags](#), and some, like [Jet Blue](#), are already partnering with CBP to implement face recognition for airplane boarding.

The Threat to Privacy and Our Freedom to Travel

We cannot overstate how big a change this will be in how the federal government regulates and tracks our movements or the huge impact this will have on privacy and on our constitutional “[right to travel](#)” and right to [anonymous association](#) with others. Even as late



CBRNE-TERRORISM NEWSLETTER – November 2017

as May 2017, CBP [recognized](#) that its power to verify the identification of travelers was limited to those entering or leaving the country. But the TSA Modernization Act would allow CBP and TSA to collect any biometrics they want from all travelers—international *and* domestic—wherever they are in the airport. That's a big change and one we shouldn't take lightly. Private implementation of face recognition at airports only makes this more ominous.

All Americans should be concerned about these proposals because the data collected—your fingerprint, the image of your face, and the scan of your iris—will be stored in [FBI](#) and [DHS](#) databases and will be searched again and again for immigration, law enforcement, and intelligence checks, including checks against latent prints associated with unsolved crimes.

That creates a risk that individuals will be implicated for crimes and immigration violations they didn't commit. These systems are notoriously inaccurate and contain out-of-date information, which poses a risk to all Americans. However, due to the fact that immigrants and people of color are disproportionately represented in criminal and immigration databases, and that face recognition systems are [less capable](#) of identifying people of color, women, and young people, the weight of these inaccuracies will fall disproportionately on them.

This vast data collection will also create a huge security risk. As we saw with the 2015 [Office of Personnel Management](#) data breach and the 2017 [Equifax breach](#), no government agency or private company is capable of fully protecting your private and sensitive information. But losing your social security or credit card numbers to fraud is nothing compared to losing your biometrics. **While you can change those numbers, you can't easily change your face.**

The shocking scale of online extremism as 300,000 videos, pages and posts removed

Source: <http://www.yorkshirepost.co.uk/news/crime/the-shocking-scale-of-online-extremism-as-300-000-videos-pages-and-posts-removed-1-8866995>

Nov 20 – A specialist anti-terror team in the UK has warned more needs to be done to tackle online extremism despite more than 300,000 videos, web pages and posts being removed after they were flagged up to internet firms.

Figures released today show the national police




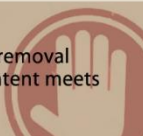
speeches calling for racial or religious violence. The statistics show that, as of last month, 299,121 pieces of material had been cleared at the instigation of the unit since its launch in 2010. Officers confirmed that the number of removals has since passed the 300,000 mark.

Detective Chief Superintendent Clarke Jarrett, of the Metropolitan Police's counter-terrorism command, said: "The 300,000 milestone is positive. It's 300,000 pieces of material not there to radicalise people. That 300,000 isn't a representation of what's out there. There's still plenty of content out there." From the start of January to the end of August this year, 43,151 pieces of content were removed at the request of the CTIRU. This was down by nearly half on the tally of 83,784 recorded in the equivalent period of 2016.

Det Chief Supt Jarrett acknowledged that removals instigated by the CTIRU have slowed, but said: "I think that's a success story because we've now got the industry into a place where they are doing more." Officers in the unit trawl the web looking for material as well as investigating referrals from the

Counter Terrorism Internet Referral Unit (CTIRU)

The CTIRU put considerable effort into removing online terrorist and extremist material. The Police rely on the public to report concerns about online content. Report it by following the 4 steps below:

1  Click on the red 'STOP' button found on Prevent Tragedies, police and other websites.	2  Click the 'Start Now' link.
3  Complete the online form.	4  The CTIRU will initiate the removal process if the reported content meets the assessment criteria.

unit reached the milestone in recent weeks, although the rate of removals prompted by its work has slowed as firms step up their own efforts.

The **Counter Terrorism Internet Referral Unit** (CTIRU) works with hundreds of organisations to remove content including propaganda and recruitment videos, images of executions and



CBRNE-TERRORISM NEWSLETTER – November 2017

public. After carrying out assessments, they contact internet providers to request the removal of harmful items. More than 300 firms have taken down material following requests from the CTIRU.

The bulk of the unit's activity deals with Islamist-related content, but it is referring more far-right material. The CTIRU was the first unit of its type in the world and UK police are keen for other countries to consider adopting the model. In recent months, companies have detailed steps they are taking to tackle terrorist content.

From January to June, Twitter removed just under 300,000 accounts for terror-related violations. YouTube has introduced "machine learning" to help identify extremist and terror-related material. Facebook has revealed it is using artificial intelligence to keep terrorist content off the site. The head of MI5 has said technology companies have an "ethical responsibility" to help confront the unprecedented threat, while Britain and France are exploring plans that could see platforms face fines if their efforts are not up to scratch.





EMERGENCY RESPONSE



Improving public safety during severe weather, other disasters

Source: <http://www.homelandsecuritynewswire.com/dr20171106-improving-public-safety-during-severe-weather-other-disasters>

Nov 06 – Our ability to observe and predict severe weather events and other disasters has improved markedly over recent decades, yet this progress does not always translate into similar advances in the systems used in such circumstances to protect lives. A more cohesive alert and warning system that integrates public and private communications mechanisms and adopts new technologies quickly is needed to deliver critical information during emergency situations. At the same time, better understanding of social and behavioral factors would improve the ways we communicate about hazards, inform response decisions such as evacuations, develop more resilient urban infrastructure, and take other steps to improve weather readiness.

The NAS [says](#) that two reports by the National Academies of Sciences propose steps to improve public safety and resilience in the face of extreme weather and other disasters.

[Emergency Alert and Warning Systems: Current Knowledge and Future Research Directions](#) examines how government systems such as Wireless Emergency Alerts (WEA) and Integrated Public Alert and Warning System (IPAWS) will need to evolve as technology advances. The transformation of these alert systems should be informed by both technological and social and behavioral sciences research, the report says.

[Integrating Social and Behavioral Sciences Within the Weather Enterprise](#) emphasizes the need for government agencies, industry, and academic institutions involved in the weather enterprise to work together to more actively engage social and behavioral scientists, in order to make greater progress in protecting life and enhancing prosperity. While efforts to improve physical weather prediction should continue, the report says, realizing the greatest return on investment from such efforts requires understanding how people's contexts, experiences, knowledge, perceptions, and attitudes shape their responses to weather risks.

Evolution of emergency alerts system based on technological changes and behavioral factors

As technology advances, government systems such as Wireless Emergency Alerts (WEA) and Integrated Public Alert and Warning System (IPAWS) will need to evolve, and their transformation should be informed by both technological and social and behavioral sciences research, says *Emergency Alert and Warning Systems: Current knowledge and future research directions*, one of the reports.

Emergency alerts and warnings are sent out by government agencies through broadcast media and WEA. But the report notes that the information ecosystem has broadened to also include a wider variety of delivery mechanisms including first-person reports on social media platforms. Private companies like Google and Facebook are also collecting information from emergency management agencies to issue notifications. The committee that conducted the study and wrote the report said government-designed systems need to fit into this larger structure of communication.

The committee envisioned an integrated alerts system that continually takes advantage of new technologies and knowledge emerging from events and research. Emergency managers should increase the use of WEA and incorporate current knowledge of how the public responds to emergency notifications to craft more effective alert messages in the near future. Those agencies and private companies responsible for evolving and implementing IPAWS and WEA should adopt newer delivery and geotargeting technologies in the next several years.

The report outlines key research questions and other areas of study. One example is to improve geotargeting by performing more research to determine the best ways to graphically display the location of an individual in a risky situation and how visualizations can be used to best illustrate the location of the message receiver relative to the area of impact. The committee also recommended exploring message characteristics like length and content when communicating about an emergency situation, how best to transmit information in multiple languages, and how to make public education campaigns regarding disaster alerts more effective.

There are also several challenges in building an effective alerts system, the report notes, such as slow adoption of new systems because of gaps in funding or expertise, the challenge of adapting to ever-changing technology, and limited opportunities for engineers, social



CBRNE-TERRORISM NEWSLETTER – November 2017

science researchers, and emergency managers to frequently interact to apply current knowledge or fill gaps in understanding.

Improving the weather enterprise with social and behavioral sciences

Weather forecasts and warnings are being made with greater accuracy, geographic specificity, and lead time, which allow people and communities to take appropriate protective measures. Yet, as recent hazardous weather events have illustrated, social and behavioral factors — including people's contexts, experiences, knowledge, perceptions, and attitudes — shape responses to weather risks, says *Integrating Social and Behavioral Sciences Within the Weather Enterprise*, the second NAS report.

The committee that conducted the study and wrote this report noted that as efforts to advance meteorological research continue, it is essential for government agencies, industry, and academic institutions, all part of the weather enterprise, to integrate social and behavioral sciences into their work. This report suggests strategies to better engage researchers and practitioners from multiple social science fields to advance those fields, to more effectively apply relevant research findings, and to foster more cooperation on this endeavor among public, private, and academic sectors.

A better understanding of social and behavioral aspects of weather readiness will help us not only to design more effective forecasts and warnings but also to reduce vulnerability and mitigate risks of hazardous weather well before an event strikes and to better support emergency management and response efforts.

The report includes a special focus on social science research related to road safety, given that road weather hazards are by far the largest cause of weather-related deaths and injuries in the United States, an estimated 445,000 people are injured and 6,000 killed annually due to weather-related vehicle accidents. Understanding why people choose to drive during hazardous weather can help in developing better strategies to discourage risky behavior. Better understanding how drivers get weather-related information can help better inform people who encounter dangerous conditions such as icy roads or low visibility while already in transit.

Many innovative social science research activities to date have made demonstrable contributions to the weather enterprise. But new insights are often not routinely applied in practice, and building a solid base of knowledge has been hampered by small-scale and inconsistent investments in these efforts. The report finds that limited support for research in this area has made it difficult to sustain a critical mass of robust studies, let alone expand research capacity. Making greater progress in advancing interdisciplinary work among physical and social science researchers also requires that meteorologists and other weather professionals have a more realistic understanding of the many disciplines and research methodologies within social and behavioral sciences; of the time and resources needed for robust research; and of the inherent limitations in providing simple, universally applicable answers to complex social questions.

NAS says that NOAA will need to play a central role in driving this research forward in order to achieve the agency's goals of improving the nation's weather readiness, the report says. The committee detailed several possible mechanisms for the agency to advance its capacity to support social and behavioral science research, including innovative public-private partnerships for interdisciplinary weather research and creating social science-focused research programs within NOAA's Cooperative Institutes. Other federal agencies that are needed as key partners in this work are the National Science Foundation, the Federal Highway Administration, and the Department of Homeland Security/FEMA.

Some examples of critical research needs highlighted in this report include: understanding how forecasters, broadcast media, emergency and transportation managers, and private weather companies interact and create and disseminate information; understanding how to better reach and inform populations that are particularly vulnerable to hazardous weather; and understanding how new communication technologies affect message design and are changing people's weather information access, interpretations, preparedness, and response.

[Emergency Alert and Warning Systems: Current Knowledge and Future Research Directions](#) was sponsored by DHS. A public webinar featuring the chair of the committee will be held at 1:30 p.m. on Wednesday, 13 December 2017. For more information or to register for the webinar, please click [here](http://alerts.eventbrite.com): <http://alerts.eventbrite.com>



CBRNE-TERRORISM NEWSLETTER – November 2017

[Integrating Social and Behavioral Sciences Within the Weather Enterprise](#) was sponsored by NOAA and the U.S. Department of Transportation. A public discussion featuring members of the committee will be held from 1-2:30 p.m. ET on Monday, 6 November 2017 at the National Academy of Sciences building. For more information or to register for the event in-person or remotely, please click here: <https://www.eventbrite.com/e/board-on-atmospheric-sciences-and-climate-fall-2017-meeting-tickets-39096052345>

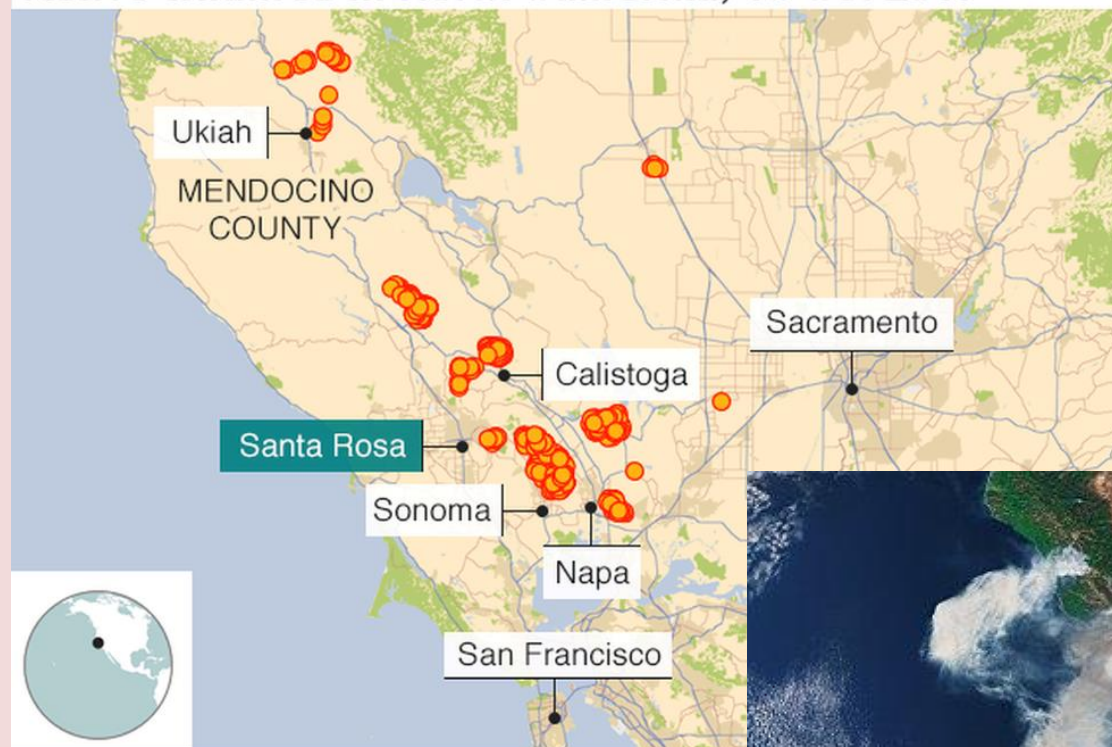
As wildfires expand, fire science needs to keep up

By Albert Simeoni

Source: <http://www.homelandsecuritynewswire.com/dr20171106-as-wildfires-expand-fire-science-needs-to-keep-up>

Nov 06 – In the month of October nearly 250,000 acres, more than 8,000 homes and over 40 people fell victim to fast-moving wildfires in Northern California, the deadliest and one of the costliest outbreaks in state history. Now is the time to wrestle with hard questions. Why did communities that were deemed safe

Active wildfires in North California, 13 Oct 2017



Source: NOAA/California Fire

suffer major damage? Should they be rebuilt in the same way? Are there better ways to fight extreme fires and limit their impact? How can emergency planners prepare better for scenarios where full evacuation is not possible?

This is a global challenge. [Brazil](#), [Indonesia](#), many parts of [Africa](#) and [Canada](#) typically experience larger wildfires (measured by area burned) than the United States on a yearly average. This year [Chile](#) and [Portugal](#) have also suffered enormous losses. Australia's [Black Saturday fires](#) in 2009 were its worst fire event ever.

Fire is part of ecosystems in much of the world, so societies must learn to live with it. But key issues are still poorly understood. What is the right degree of fire management to decrease the impact of catastrophic fires? What is the most efficient way to protect the wildland-urban interface – the area where houses meet or intermingle with undeveloped wildland vegetation? And what is the best way to evacuate?



CBRNE-TERRORISM NEWSLETTER – November 2017

In my view and that of other researchers, many countries, including the United States, are [underfunding research](#) designed to answer these questions.

**Moving into harm's way**

Wildfires are increasing and affecting more areas worldwide. One cause is urban sprawl and the dramatic expansion of the wildland-urban interface. In the 1990s this zone increased by almost 11 percent in California, Oregon and Washington, adding [over 1 million housing units](#) – mostly in areas of moderate to high fire risk. At the same time, climate change is creating worse and more frequent wildfire conditions. No one can control the weather, which is likely to become more extreme, but it is critical to do more to understand [vulnerabilities that exist at the wildland-urban interface](#). Research has identified some factors that create these risks, including the ease with which homes ignite and the spread of fire between structures. Developing solutions will require quantifying the risks. It is also important to evaluate how vegetation treatment, structure hardening and better community design can [decrease the likelihood of structural ignition and fire spread](#).

Winds, flames and fuels

U.S. building and fire protection standards and regulations have improved in the last 10 to 15 years, particularly in California, but many communities are still extremely vulnerable. Best practices, such as the National Fire Protection Association's [Firewise](#) USA program and California's [Fire Safe](#), are a good start but should be expanded, based on research.

Understanding of vulnerabilities at a structural level is improving but not sufficient yet. Once fire moves from wildlands into developed areas, flames are fueled by engulfed homes and structures, creating conflagrations. For example, the California fires consumed entire neighborhoods as flames spread unhindered from one flammable element to another. This pattern has also been observed in [many other locations](#).

[Better community design](#) could help prevent this domino effect, averting massive property losses and evacuations. Communities should contain patchworks of flammable fuels such as vegetation, houses and cars, interspersed with less flammable and nonflammable areas such as parking lots and areas cleaned of vegetation. This strategy can decrease fire intensity, slow down fires and break down large fire fronts into smaller fingers that are easier to fight.

Another priority is the role of flammable building materials. Structural ignition often starts with [firebrands](#) – pieces of burning wood that are lofted by winds, and can spread wildfire past barriers and firebreaks – but scientists are still working to [quantify their impact](#).

Many interacting factors influence whether and how wildfires will spread, including fire intensity, wind intensity, the quantity of firebrands that land on structures, the heat that



CBRNE-TERRORISM NEWSLETTER – November 2017

impacts structures, how structures ignite, the distance between structures and vegetation, and the distance between structures. Researchers should aim to design suites of engineering solutions that will be versatile enough to adjust to specific scenarios and quantified exposures. They should include small-scale steps, such as removing flammable vegetation, pruning trees, using less-flammable construction materials, and dealing with identified vulnerabilities such as [fences](#). And they should extend to larger-scale strategies, such as breaking up wildfire fronts, slowing down fire spread and redesigning communities.

Major costs, modest funding

U.S. fire research is funded by the U.S. [Forest Service](#), the [National Institute of Standards and Technology](#) and other federal agencies. Universities receive funding through the [Joint Fire Science Program](#), which is jointly funded by the Interior Department and the Forest Service, and indirectly through other agencies such as the National Science Foundation, the [Defense Department's environmental research programs](#) and NASA.

Federal funding for fire research pales compared to the cost of fighting wildfires and the economic damage they cause. For example, in 2017 the Forest Service received [about US\\$27 million](#) for the National Fire Plan Research and Development Program and the Joint Fire Science Program, while the Interior Department received [about \\$6 million](#) for the Joint Fire Science Program. President Trump's 2018 budget request would [terminate Forest Service's participation in the Joint Fire Science Program](#) and reduce the Department of the Interior's funding for the program to [\\$3 million](#), which would mean no new projects and topics funded. Many members of the research community are [concerned about this lack of investment](#). For comparison, the Forest Service and Interior together spent [nearly \\$2 billion in 2016](#) fighting wildfires. The Forest Service alone has spent [over \\$2 billion](#) in this fiscal year on wildland fire suppression. And preliminary damage estimates for the California wildfires range from [\\$1 billion to \\$6 billion or more](#).

Similar pressures undercut funding for wildfire prevention in [Portugal](#) after its 2011-2014 recession. And the European Union stopped funding basic science related to fire dynamics and wildland-urban interface fires almost a decade ago, focusing instead on applied technological projects and more general research on natural disasters. Funding for firefighting has also declined in Russia, where environmental groups claim that the number of fires is [significantly underreported](#).

Fire conditions are constantly evolving, and basic research coupled with engineering solutions must keep up. Designing more resilient communities and infrastructure and protecting people more effectively are not onetime goals – they are constant. Currently nations are failing to meet the challenge, and impacts on communities are increasing.

Albert Simeoni is Professor of Fire Protection Engineering, Worcester Polytechnic Institute.

The Dopplerian Resonance Effect on Continual Preparedness

By Adam Montella

Source: <https://www.domesticpreparedness.com/healthcare/the-dopplerian-resonance-effect-on-continual-preparedness/>

Oct 2008 – There are several events in recent memory of such national significance that they have caused a lasting as well as dynamic change from “business as usual” in the disaster-response arena. Hurricane Andrew spawned the Stafford Act in 1988, for example, forever changing how the Federal Emergency Management Agency (FEMA) and other agencies respond to disasters. In 1996, the Nunn-Lugar-Domenici Act, based on the heightened threat of terrorism in the United States, gave birth to the Domestic Preparedness Program and the Office for Domestic Preparedness. However, the Stafford Act did not foresee the massive breakdowns that occurred between the states, the federal government, and local communities in response to Hurricane Katrina, and the Nunn-Lugar-Domenici Act did nothing to prepare for the massive resource coordination effort needed to respond to the 11 September 2001 terrorist attacks and to the release of anthrax at several offices on Capitol Hill and the testing of thousands of suspected packages with “white powdery substances” that followed shortly thereafter. It seems, unfortunately, that the further the American people get from events like September 11, the more complacent and unguarded they become – and vigilance seems to be on pause



CBRNE-TERRORISM NEWSLETTER – November 2017

in personal and corporate as well as government planning. Even the threat of a pandemic influenza, a frightening topic only a year ago, barely gets a mention today outside of planning circles, showing up, if at all, as a distant blip on the nation's collective radar screen. This is a far cry from the period immediately after the 9/11 attacks, when there was a surge of family-created disaster plans, businesses hosted workshops to educate their employees on what to do in an emergency, and there was more coordination between and among all levels of government, private industry, and individual citizens.

Today, there are several initiatives focused on public-health and healthcare-response planning, the penultimate area of critical-infrastructure focus for ensuring population-based safety and survivability under conditions of severe environmental duress. **The Joint Task Force National Capital Region - Medical (JTF-CapMed) initiative** represents an effort to assist the nation's civilian and military public-health and healthcare infrastructure to join forces in a network-centric, collaborative architecture for incident management and response. This effort might well serve as a national template for private industry to enter into an even greater cooperative and collaborative preparedness and response framework. If successful, JTF-CapMed would certainly represent a highly repeatable approach to regional-preparedness and response-planning efforts.

Money Well Spent; Capabilities Well Achieved

It seems clear that all of the hundreds of millions of dollars that have been spent on equipment and interoperability initiatives in recent years have significantly improved the day-to-day readiness capabilities of local communities throughout the United States. However, those capabilities have never been consolidated in a true regional or nationally coordinated response plan fully based on accepted NIMS (National Incident Management System) principles. There are large stores of emergency equipment now in place throughout the country, to cite one example of increased capabilities, but one could challenge most jurisdictions to specifically identify where that equipment is stored, and whether it is operational or not.

Corporate business planning, moreover, is now seen as a luxury in today's unstable economy. In addition, many if not all families and individual citizens seem to be motivated only by the most recent disaster affecting them personally. Anyone asking a New Yorker if his city has a hurricane plan in place, and then asking the same question of a resident of New Orleans would almost certainly receive two different answers.

Which brings up a reasonable but absolutely necessary question: Why are the American people not better prepared today? One at least partial answer is what might be called the "Dopplerian Resonance of Disasters" – a term coined by the former chief medical planner for the U.S. Department of Defense, Pietro (Peter) Marghella. As he explains it, "Much like a train speeding toward a station, early warning systems, intelligence resources, and detection and surveillance assets allow us to *feel* the

vibrational resonance of an approaching disaster. We, of course, can choose to take actions to improve our posture of preparedness once the vibration is felt.

"Or we can choose to ignore it," he continues, "and hope that we won't be standing on the track when the 'train' explodes by us. Unless [we ourselves] ... have been hit by the disaster ... we tend to remember the event only to the extent that we feel that vibration; the longer the disaster moves away from us in time and space, the more likely we are to drop our guards and give less effort to preparing for the inevitable next disaster."

A Paradigm Shift to True Interoperability

The best and perhaps only way to be *better* prepared, though, is to be *always* prepared. It is not sufficient simply to write a comprehensive emergency-management plan, or a medical-response plan, publish it, and then file it away. The plan starts to become outdated the second it is printed. It is time, therefore, to embrace the idea of "Continual Preparedness."

But Continual Preparedness takes planning, a lot of planning, and the integrated response that follows it, to an entirely new level. It also assumes the involvement of all stakeholders ranging from government agencies and non-profit organizations to private industry and individual citizens. Finally, for the plan to be truly effective and ready for use in an actual emergency, it must be kept as current as possible -- or it will be forgotten just as quickly as the disaster that gave birth to the plan in the first place.

William (Bill) Josko, Vice President of Previsar Inc. and a public-safety and homeland-security software



CBRNE-TERRORISM NEWSLETTER – November 2017

expert, commented as follows on the current U.S. state of interoperability: “Technologies exist today that effectively bridge the chasm of collaboration and true interoperability in both communications and data environments.” Josko further explained that having such standards in place as the National Information Exchange Model (NIEM), the Common Alerting Protocol (CAP), and the Information Sharing Environment (ISE), coupled with enabling technologies such as XML, Web Services, and other types of middleware – all operating within a systems-oriented architecture – allows true interoperability to finally become reality.

From a technical as well as technological perspective, therefore, there probably has never been a better time for stakeholders at all levels of society to truly interoperate and collaborate.

However, in Josko’s opinion, technology is not the real issue but, rather, the existing “siloization” of those multiple stakeholders -- in both the public and private sectors -- that inhibits collaboration toward unified planning and response that presents the greatest challenge. Combining what Marghella and Josko have to say lends itself perfectly to the concept of Continual Preparedness. The United States must align people, processes, policy, and technology to, as Marghella often says, “Marry the planner’s art with the planner’s science.” In short, to truly achieve a state of Continual Preparedness the United States must achieve a major paradigm shift characterized by meta-leadership among all of the stakeholders involved.

Adam Montella is Vice President of Homeland Security and Emergency Management Services for Previsar Inc. and a nationally known emergency-management and homeland-security professional with more than 23 years direct experience in both government and the private sector. He served as the first general manager of emergency management for the Port Authority of New York and New Jersey in the period following the 11 September 2001 terrorist attacks and has served in many other emergency-management positions at all levels of government. A former member of the House Operations Recovery Team of the U.S. House of Representatives and of numerous local, state, national, and international emergency management associations, he also is a well known public speaker in his chosen field and a former recipient of Harvard University’s prestigious Innovations in American Government Award.

Worst-case scenarios: Why we should welcome warnings

Source: <http://www.homelandsecuritynewswire.com/dr20171108-worstcase-scenarios-why-we-should-welcome-warnings>

Nov 08 – Nuclear accidents. Sea level rise. Terror threats. The world is full of potential catastrophes, but most of the time, most of us are oblivious to them.



Still, at times, experts warn the rest of us about these potential crises. Sometimes those warnings work, but many times they go unheeded. Why do we ignore information we could use to stave off a disaster? Prominent national security expert Richard Clarke SM '79 [weighted in](#) on this issue at MIT’s latest Starr Forum event last Wednesday, making the case that we should be more receptive to the possibility of dire news, as well as more systematic about analyzing it.

The [Greek] mythological Cassandra who has the ability to see the future

Clarke, the former chief counter-terrorism advisor on the National Security Council, expanded on



CBRNE-TERRORISM NEWSLETTER – November 2017

ideas in his new book, [*Warnings: Finding Cassandras to Stop Catastrophes*](#), asserting that specialists in a range of fields can “see the thing buried in the data that other people don’t see. They see it first.”

Clarke called these people “Cassandras,” after the figure in Greek mythology who could see the future, and described them as experts with accumulated knowledge and a willingness to explore worst-case scenarios.

“It just can’t be any old person off the street saying the sky is falling,” Clarke said. “It has to be a recognized, acknowledged expert in the field they were giving the warning in. ... They had to have studied it and been data-driven.”

Prove me wrong

Examples of this dynamic abound. Engineers warned that Japan’s nuclear power industry was vulnerable to natural disasters well before the Fukushima earthquake and tsunami of 2011. Experts stated that New Orleans was vulnerable to flooding before Hurricane Katrina hit in 2005. Climate scientists, for decades, have warned the world that global warming could upend life as we know it.

And Clarke, for his part, gained a significant public profile after being one of the U.S. security officials most concerned about the threat of the al Qaeda terror group before the attacks of Sept. 11, 2001.

But plenty of dire-sounding warnings can also be unfounded and ultimately incorrect. So how can leaders — in government, business, or elsewhere — distinguish between legitimate fears and simplistic scare-mongering?

To Clarke, a person with a legitimate warning to offer will be willing to have their ideas tested by others: “Cassandras repeatedly say, ‘Well, I gave my data to other experts in the field and said, prove me wrong, and none of them could. They could never prove my data wrong.’”

Why not act?

But if experts are often raising concerns, why do those warnings get ignored? Clarke emphasized that being quick to recognize concerns produces its own set of problems, starting with a lack of consensus.

When experts are “yelling to a decision maker, ‘There’s a problem,’ the decision maker says, ‘Yeah? Who else believes you? What other experts in the field agree?’”

Then too, Clarke said, data-based concerns over catastrophes can be ignored due to what he calls “first occurrence syndrome,” namely, the fact that many potential problems have “never happened before, in the memory of the people involved.” New Orleans, for example, had never previously flooded to the degree that it did due to Hurricane Katrina. It is easier to imagine that history will continue within its recent bounds.

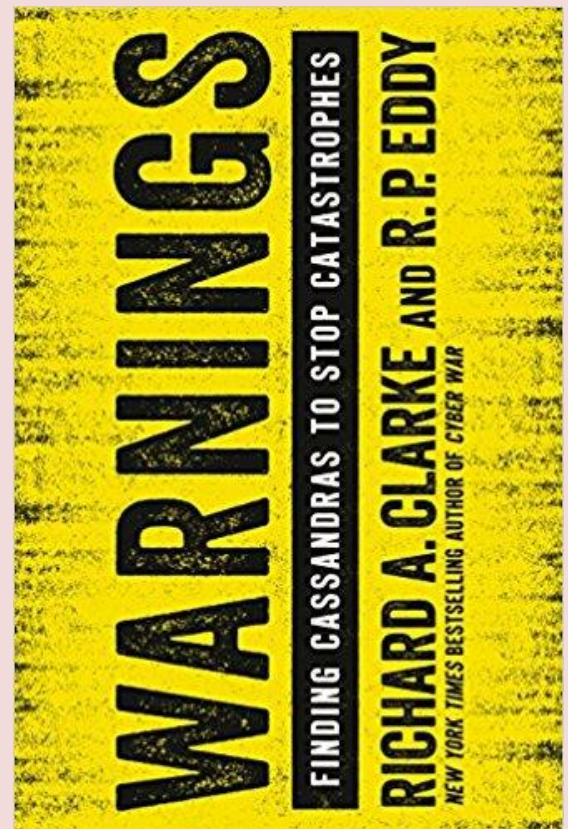
Meanwhile, Clarke noted, there can be a “diffusion of accountability” in organizations. One data scientist repeatedly told the firm Equifax recently that it was vulnerable to being hacked, he said. But the responsibility for acting on that was essentially distributed among several people — which can lead to institutional inertia.

Additionally, Clarke added, to stave off disaster, especially in matters related to climate change, “You might have to do something ideologically abhorrent to you. You might have to raise taxes or try carbon capture or enact regulations.” Thus solutions mean to pre-empt catastrophes of all kinds can languish.

See the sea rise

The Starr Forum consists of a series of public discussions, sponsored by MIT’s Center for International Studies, focused on global security issues and other matters of international politics. About 125 people attended the event Wednesday, which was open to the public.

Clarke’s remarks were followed by a dialogue with counterintelligence expert and Center for International Studies Fellow Joel Brenner, as well as a question-and-answer session with the audience.



CBRNE-TERRORISM NEWSLETTER – November 2017

In his remarks, Clarke observed that being a “Cassandra” can take a heavy psychological toll on experts who find their ideas marginalized.

“A lot of these people get agitated when they are ignored,” he said.

Brenner largely concurred, but wryly noted that “a lot of these people have a special talent for burning bridges” within the organizations they are serving. Still, Brenner noted, the complications of contemporary society and technology mean it is generally safe to assume, at any given time, that “something is going seriously wrong somewhere.”

Asked to produce a hierarchy of issues for us to worry about, Clarke emphasized the vast problems that sea level rise, as a product of climate change, could create in the decades ahead. Rather than the consensus estimate of 3 meters of sea level rise by the year 2100, Clarke stated, we could see 6 to 9 meters of sea level rise by 2050 or 2075.

“Think about the economic, political, social implications of that,” Clarke said. “Some countries disappear. Mass migrations of people.” He also cited the potential for economic “collapse” in some areas.

Still, Clarke did try to inject some hope into the proceedings.

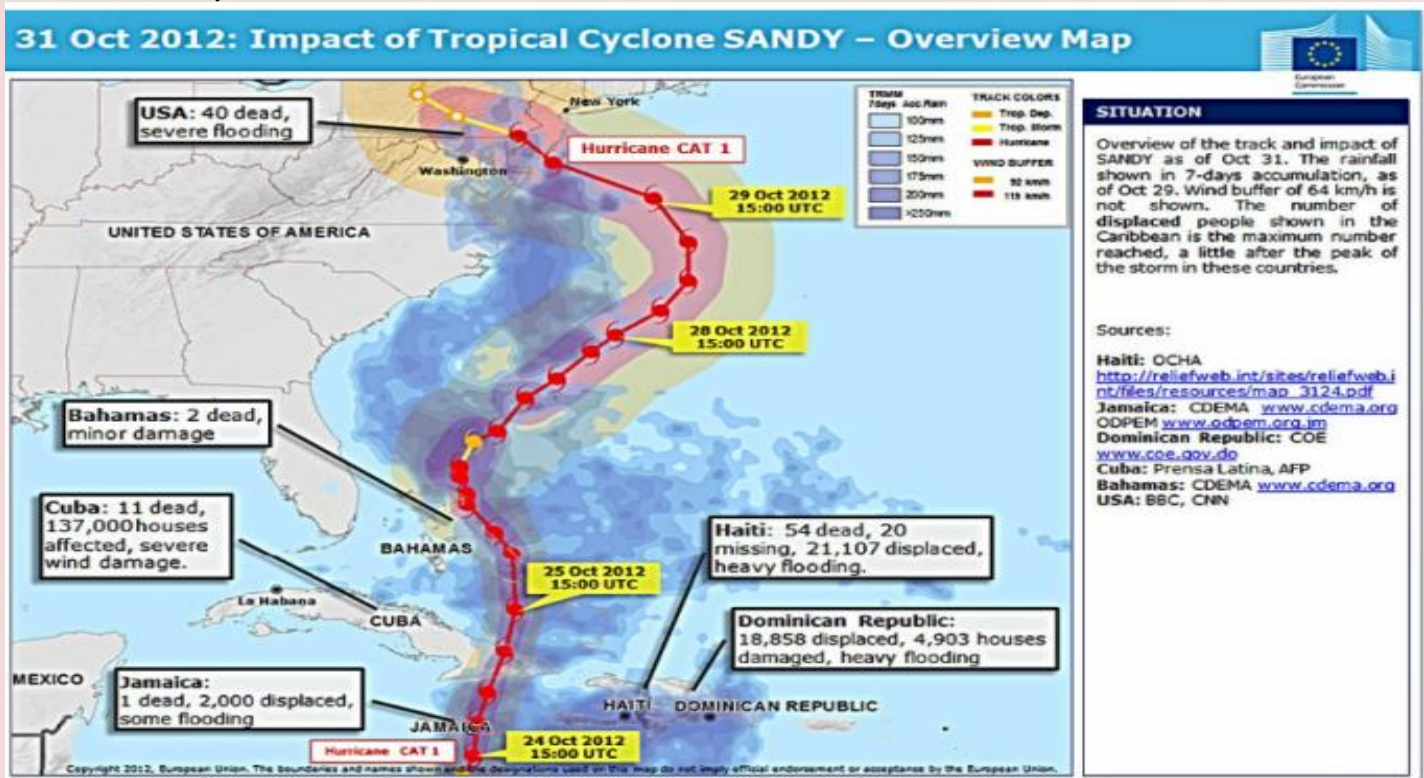
“I believe in good government’s ability to be rational and save the world from some of these disasters,” Clarke said, adding: “I think it’s an optimistic book, because it holds out the hope that if you had systematic thinking [and] rational analysis, systems thinking, if you want to call it that, we could see problems coming, and stop them from being really big problems.”

Sandy five years later. What have we learned?

Source: <http://www.homelandsecuritynewswire.com/dr20171108-sandy-five-years-later-what-have-we-learned>

Nov 08 – Five years ago, Post-tropical Cyclone Sandy struck at high tide, driving catastrophic storm surge into coastal New Jersey and New York unlike anything seen before. Thirty-four New Jersey residents lost their lives. Hundreds of thousands of homes and businesses were destroyed, causing over \$62 billion in damage.

Five years later some areas have recovered. Some have not.



“Nature is ferocious, and a major coastal storm can devastate a community in a matter of hours. Severely impacted communities need both patience and inspiration to recover:



CBRNE-TERRORISM NEWSLETTER – November 2017

patience with the time it takes to repair the economic and social fabric that sustains communities, and inspiration to envision and plan for a future that is less vulnerable to coastal storms,” says Darlene Finch, Mid-Atlantic Regional Coordinator with NOAA’s Office for Coastal Management.

Many community leaders believe super storms are the new norm, and are increasing efforts to make communities more resilient—a critical component of all recovery efforts. NOAA [points](#) to two examples:

- ◆ New Jersey’s [Brigantine Island community](#) used the recovery phase as an opportunity to elevate the road off the island, strengthen barriers along the oceanfront and bayside, and improve zoning and floodplain ordinances.
- ◆ New Jersey’s coastal management program developed a [Getting to Resilience](#) program to help communities improve hazard preparedness. As a result, many communities instituted new policies that keep people and infrastructure safer, and also resulted in cost reductions for flood insurance premiums.

“Sandy’s devastation provided an opportunity to make impacted communities more resilient,” says Finch. “At NOAA, we are committed to providing data, tools, and information that help communities recover. Our resources enable them to work side-by-side with partners and community leaders. They can then transfer their ideas and lessons learned to other communities facing similar circumstances.”

The Sphere Project

Source: <http://www.sphereproject.org/>

The Sphere Project is a voluntary initiative that brings a [wide range of humanitarian agencies](#) together around a common aim - to improve the quality of humanitarian assistance and the accountability of



humanitarian actors to their constituents, donors and affected populations.

The [Sphere Handbook, Humanitarian Charter and Minimum Standards in Humanitarian Response](#), is one of the most widely known and internationally recognized sets of common principles and universal minimum standards in life-saving areas of humanitarian response.

Established in 1997, the Sphere Project is not a membership organization. Governed by a Board composed of representatives of global networks of humanitarian agencies, the Sphere Project today is a vibrant [community](#) of humanitarian response practitioners.



ICI
International
CBRNE
INSTITUTE



ASYMMETRIC THREATS



Global warming is here, caused by human activity: Massive federal government report

Source: <http://www.homelandsecuritynewswire.com/dr20171103-global-warming-is-here-caused-by-human-activity-massive-federal-government-report>

Nov 03 – The White House allowed the release on Friday of a report by U.S. government's scientists – the [Climate Science Special Report](#) – which offers voluminous scientific evidence that climate change is real, it is already here, and that it has been caused – and is being exacerbated – by human activity. The report, which is mandated by Congress, is the most comprehensive report on climate change ever produced.

The study, noting that the planet is now the warmest it has been in the history of modern civilization, says that “it's extremely likely that human activities, especially emissions of greenhouse gases, are the dominant cause of the observed warming since the mid-twentieth century.”

“For the warming over the last century, there is no convincing alternative explanation supported by the extent of the observational evidence,” the report said.

Referring to the rapidly rising levels of greenhouse gases in the atmosphere, the report states: “there is no climate analog for this century at any time in at least the last 50 million years.”

USA Today [reports](#) that the report, which is the first of two volume of the National Climate Assessment, is federally mandated, and is prepared by the U.S. top scientists every four years for the president, the

Congress, and the public.

This National Climate Assessment is the fourth such report. It has been researched and assembled by a team of more than 300 experts from thirteen government agencies who have analyzed more than 1,500 scientific studies and reports. They were guided by a 60-member Federal Advisory Committee.

The report was also peer reviewed by the National Academy of Sciences.

The second volume of the assessment, focusing on the regional impacts across the United States, was released Friday as a draft for public comment.

Combined, the two documents total more than 2,000 pages.

The contents of the report and the scientific evidence it presents flatly contradict claims by President Donald Trump that global warming is “a hoax” invented by the Chinese, and assertions by members of his team, especially by Scott Pruitt, the director of the Environmental Protection Agency, who have persistently downplayed the contributions human activity makes to climate change and questioned the ability of scientists to predict the effects of global warming.

Trump earlier this year announced that the United States would withdraw from the Paris climate agreement, which requires signatory nations to set and achieve ambitious targets to reduce

the greenhouse gases that cause global warming.

The EPA under Pruitt is in the process of dismantling the main environmental regulations written under Presidents George W. Bush and Barack Obama, and the EPA, on Pruitt's instructions, has removed references to “climate change” and “global warming” from the agency's website.

The *Washington Post* [reports](#) that the EPA also has altered parts of its website containing detailed climate data and scientific information. In April the agency took down pages that had existed for years and contained a wealth of information on the scientific causes of global warming, its consequences and ways for communities to mitigate or adapt. The agency said that it was making changes to better reflect the new administration's priorities and that any pages taken down would be archived. Other departments have also removed climate-change information and documents from their websites: The Interior Department's Bureau of Land Management, for example, no longer



CBRNE-TERRORISM NEWSLETTER – November 2017

provides access to documents assessing the danger that future warming poses to deserts in the Southwest.

Rick Perry, the secretary of energy, has raised the possibility of offering government subsidies to coal production, as coal is losing the battle in the market place to cleaner sources of energy such as natural gas and renewables.

Political appointees in different departments have altered the wording of their departments' news releases if those releases made references to climate change, and blocked civil servants from speaking about their conclusions in public forums.

The report's lead author, David Fahey of NOAA, noted that there are no policy recommendations in the report, only scientific information. He added that there was also no interference from policymakers.

Virginia Burkett, a scientist with the U.S. Geological Survey and acting chair of the subcommittee on Global Change Research, said that the White House Office of Science and Technology signed off on the report, said.

Among the report's findings:

- ◆ Global average sea level has risen by about 7–8 inches since 1900, with almost half (about 3 inches) of that rise occurring since 1993.
- ◆ Global average sea levels are expected to continue to rise — by at least several inches in the next 15 years and by 1–4 feet by 2100. A rise of as much as 8 feet by 2100 cannot be ruled out.
- ◆ Heavy rainfall is increasing in intensity and frequency across the United States and globally and is expected to continue to increase.
- ◆ The incidence of daily tidal flooding is accelerating in more than 25 Atlantic and Gulf Coast cities.
- ◆ Heatwaves have become more frequent in the United States since the 1960s, while extreme cold temperatures and cold waves are less frequent.
- ◆ The incidence of large forest fires in the western United States and Alaska has increased since the early 1980s and is projected to further increase.
- ◆ Annual trends toward earlier spring melt and reduced snowpack are already affecting water resources in the western United States.

The report noted that the concentration of global atmospheric carbon dioxide has now passed 400 parts per million. The last time such concentrations were reached was about three million years ago, when both global average temperature and sea level were significantly higher than today.

The report, for the first time, also included a list of what it calls climate-related “surprises,” or unanticipated changes, in which tipping points in the Earth's systems are crossed or climate-related extreme events happen at the same time, creating “compound extreme events,” multiplying the potential damage and destruction. These changes include large-scale shifts in major worldwide climate patterns that would wreak havoc on the global climate system.

The report concludes that “climate models are more likely to underestimate than to overestimate the amount of long-term future change.”

“The Climate Science Special Report is the most up-to-date comprehensive report on climate science available right now anywhere on the planet,” Robert E. Kopp, a climate and sea-level rise expert at Rutgers who helped write the report, told *USA Today*. “It confirms that climate change is real, occurring today, and principally caused by human emissions.”

Rachel Licker, senior climate scientist at the Union of Concerned Scientists, said:

The draft NCA highlights the significant impacts climate change is already having around the country. Those impacts, including on our health and economy, will likely worsen unless we take strong steps to limit global warming emissions, and adequately prepare and protect communities.

As with the earlier installments of the NCA, the latest report is making its way through rigorous scientific review that ensures a strong, accurate product and complete transparency. Before the report can be finalized in 2018, it will be reviewed by hundreds of independent scientists spanning disciplines and fields of expertise, including those from the National Academy of Sciences. It will also incorporate public comments received, which will likely total into the thousands.

The assessment is like a doctor's report that evaluates a patient's vital signs and uses that information to diagnose a medical condition. In this case the medical condition is climate change and the symptoms are rising temperatures, higher sea



levels and more extreme weather events. Experience tells us, and the Climate Science Special Report confirms, the United States is experiencing recurring heat waves, heavy rainfalls, more intense wildfires, and greater flooding from rising seas.

The Climate Science Special Report also reaffirms that humanity's emissions of heat-trapping gasses are the primary driver of the recent rise in global temperatures. It finds that with significant reductions in emissions, global temperature rise could be limited to less than 3.6 degrees Fahrenheit above pre-industrial levels, consistent with the long-term temperature goal of the Paris Agreement.

Unlike a physician, the climate assessment stops short of offering up a specific prescription or treatment plan. Instead, the American public must hold legislators and policy-makers accountable for taking action commensurate with the problem.

The report could have considerable legal and policy significance, providing new and stronger support for the EPA's greenhouse-gas "endangerment finding" under the Clean Air Act, which lays the foundation for regulations on emissions.

"This is a federal government report whose contents completely undercut their policies, completely undercut the statements made by senior members of the administration," Phil Duffy, director of the Woods Hole Research Center, [told](#) the *Washington Post*.

— Read more in [Climate Science Special Report, Fourth National Climate Assessment, Volume 1 \(U.S. Global Change Research Program, 2017\)](#).

Climate change and nuclear threats are twins

Source: <http://www.eco-business.com/news/climate-change-and-nuclear-threats-are-twins/>

Nov 20 – Climate change and nuclear threats feed off each other and should be treated in unison, an influential US think-tank says.

Climate change and nuclear threats are closely linked and must be tackled together, US experts say.

The warning comes from a working group chaired by the [Center for Climate and Security](#) (CCS), a non-partisan policy institute of security and military experts (many of them high-ranking former members of the armed forces), in a [report](#) which offers a framework for understanding and addressing the distinct problems together.

The report is published as this year's [UN climate summit](#) draws to a close in Bonn in the aftermath of [President Trump's tour of Asia](#), during which nuclear weapons issues featured prominently.

[Professor Christine Parthemore](#), a former adviser to the US defence department, co-chairs the working group. She told the Climate News Network:

"Simultaneous effects of climate change, tough social or economic pressures, and security challenges could increase the risk of conflict among nuclear weapon-possessing states, even if that conflict stems from miscalculation or misperception. India and Pakistan are major concerns.

"They are grappling with water stress, deadly natural disasters, terrorism, and numerous other pressures. At the same time, the types of nuclear weapons they are developing and policies on command of those weapons are raising tensions between them.

"Our group believed this is a recipe for not only increasing the risk of conflict, but for raising the risk of such a conflict escalating to the nuclear realm.

"Big picture: nuclear nonproliferation regimes and international climate change cooperation help underpin the global order. They are stabilising forces, and if we don't continue strengthening them, we may see a less predictable global security environment.

"This is especially dangerous in times like these when some countries are more actively flaunting their nuclear threats toward one another. North Korea has been the most active in that regard."

The authors say countries such as Nigeria, Jordan, Egypt and Saudi Arabia are dealing simultaneously with a range of interdependent internal pressures – including climatic, economic, security, and environmental demands – as they pursue nuclear energy.

Simultaneous effects of climate change, tough social or economic pressures, and security challenges could increase the risk of conflict among nuclear weapon-possessing states, even if that conflict stems from miscalculation or misperception.



CBRNE-TERRORISM NEWSLETTER – November 2017

Christine Parthemore, co-chairperson, Center for Climate and Security

Reactor safety

Bangladesh is coping with sea-level rise and changing Himalayan glacial patterns, and with terrorism and overpopulation. The report says these stresses could affect the security and safety of the nuclear reactors being built in the country with Russian help.

It says extreme heat, flooding, sea level rise and natural disasters are already affecting power stations and could knock out nuclear installations in countries already short of electricity and facing social or political pressure.

The same dilemmas could face sites handling nuclear weapons.

Concerns about nuclear security and proliferation could help countries to rely instead on fossil fuels and maintain their high dependence on them, “making dangerous, business-as-usual climate change scenarios more likely”.

And it says people forced into [migration](#) by climate change or other factors can affect security and nuclear stability.

The report says it is important to develop technologies to help countries which seek to introduce nuclear energy, including the safest reactor designs, modern security and monitoring systems and strong climate modelling abilities.

New risks

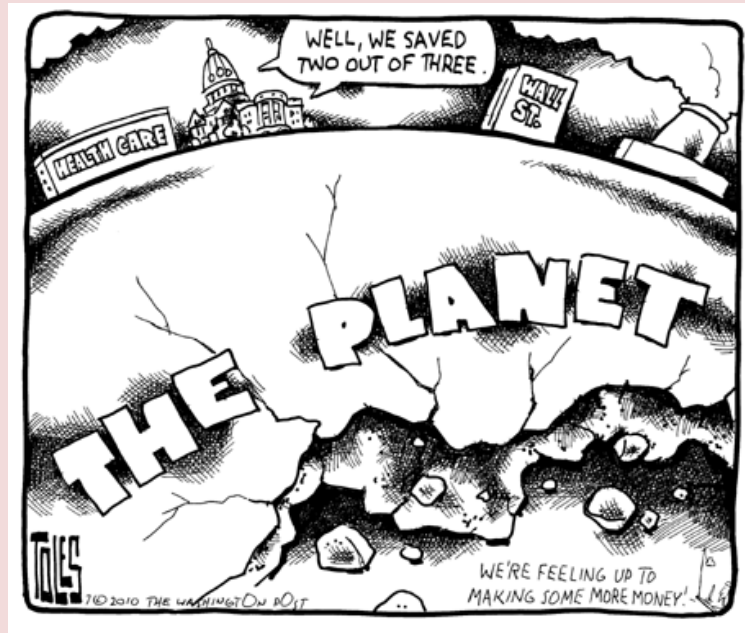
It says this is especially critical in the potential crisis regions where combining security, climate, and nuclear risks must be addressed urgently: South Asia, the Middle East, the South China Sea and Central and North Africa.

The report also says there is mounting evidence that various security challenges, climatic trends and nuclear issues are combining in new and potentially high-risk ways.

Mapping and addressing this complexity is critical for protecting US security interests not only in these crisis regions, but across the Indo-Asia-Pacific and Europe as well.

It urges the US to develop realistic planning, better communication about nuclear and climate risks, and education for policymakers about practical ways they can protect America’s capacities for coping with these challenges.

The report suggests that US leaders should encourage more robust engagement between public and policymakers on risks like nuclear conflict and climate change, and should convey risks in ways that people can relate to, for example emphasising ways to reduce threats to vulnerable infrastructure.

**The threat of crowdsourced terrorism**

Source: <http://www.thehindu.com/todays-paper/tp-national/tp-karnataka/the-threat-of-crowdsourced-terrorism/article20554149.ece>

Nov 20 – As leading cybersecurity experts from India, the United States and Israel took to the stage on the second day of the Security 360 conference in the city on Saturday, the consensus that emerged was that “crowdsourced” or “direct-to-home” terrorism, presently practised by the Islamic State (IS), was likely to dominate the rest of the 21st century.

M.K. Narayanan, the country’s National Security Adviser between 2005 and 2010, said more often than not, most “lone wolf attacks” on foreign soil were remotely plotted by IS handlers from thousands of miles away. “The global diffusion of IT, transport and finance networks will make the asymmetric threats by non-state actors like IS more potent. IS has been exploiting

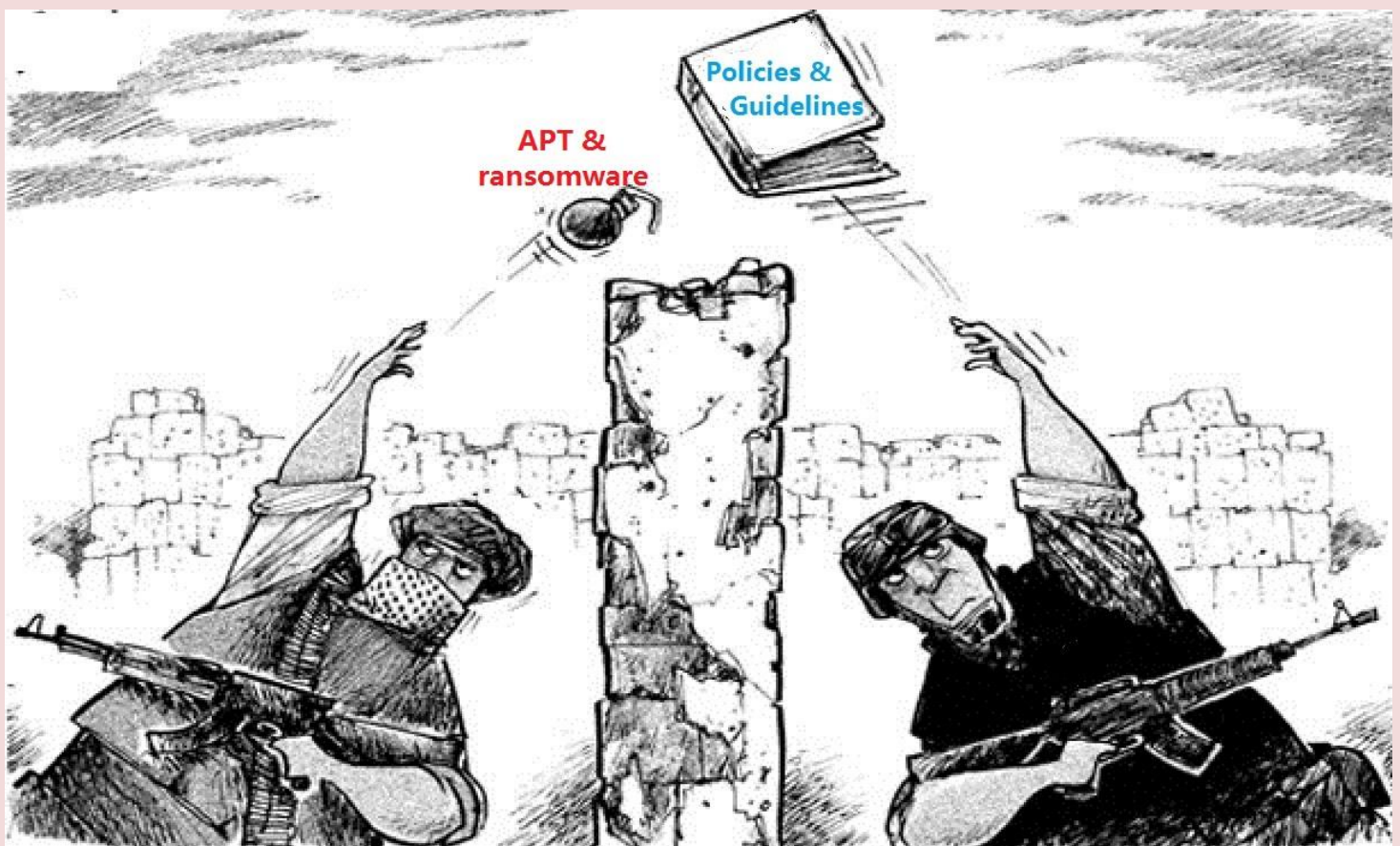


CBRNE-TERRORISM NEWSLETTER – November 2017

direct-to-home jihad and we will only see more of it. We will see more of cyber planners and virtual coaches,” he said.

Michael Chertoff, the second U.S. Secretary of Homeland Security and served under President George W. Bush, said the time of grand strategies by powerful nation states was a thing of the past. He said it was now the age of little strategies, as terrorism has gone the crowdsourcing way. “Nation-states and their intelligence agencies may find themselves severely challenged to counter such terrorism. Local authorities and communities will be called upon to get more involved in security. Intelligence agencies cannot know what is happening in your coffee shops,” he said.

According to Mr. Narayanan, asymmetric threats are likely to cooperate and network with insurgencies, leading to considerable geographical area control. He predicted that attacks on critical infrastructure would enter the cyber warfare phase, covering nation-states and trying to cripple the defences of other countries including satellites, missiles and nuclear capabilities.





BUSINESS CONTINUITY



Business Interruption

Disaster Event

Business continuity and disaster recovery planning: The basics

By Derek Slater

Source: <https://www.csoonline.com/article/2118605/disaster-recovery/business-continuity-and-disaster-recovery-planning-the-basics.html?page=2>

It bears repeating: Information systems are certainly central to today's business operations. However, an IT-only BCDR plan is hardly a plan at all. The same holds true for a facilities-only plan. Understanding the full array of assets, people, systems, and processes that make your business run is the key to success. More and more organizations are creating [Enterprise Risk Management departments](#) or programs, and that is a natural fit for business continuity efforts.

Can we outsource our contingency measures?

[Disaster recovery services](#)—offsite data storage, mobile phone units, remote workstations and the like—are often outsourced, simply because it makes more sense than purchasing extra equipment or space that may never be used. In the days after the Sept. 11 attacks, disaster recovery vendors restored systems and provided temporary office space, complete with telephones and Internet access for dozens of displaced companies.

How do you convince the CEO or the board of the need for disaster recovery plans and capabilities?

Hager advised [chief security officers](#) to address the need for disaster recovery through analysis and documentation of the potential financial losses. Work with your legal and financial departments to document the total losses per day that your company would face if you were not capable of quick recovery. By thoroughly reviewing your business continuance and disaster recovery plans, you can identify the gaps that may lead to a successful recovery. Remember: Disaster recovery and business continuance are nothing more than risk avoidance. Senior managers understand more clearly when you can demonstrate how much risk they are taking."

Hager also says that smaller companies have more (and cheaper) options for disaster recovery than bigger ones. For example, the data can be taken home at night. That's certainly a low-cost way to do offsite backup.

Some of this sounds like overkill for my company. Isn't it a bit much?

The elaborate machinations that USAA went through in developing and testing its contingency plans might strike the average CSO (or CEO, anyway) as being over the top. And for some businesses, that's absolutely true. After all, HazMat training and an evacuation plan for 20,000 employees is not a necessity for every company.

Like many security issues, continuity planning comes down to basic [risk management](#): How much risk can your company tolerate, and how much is it willing to spend to mitigate various risks?

In planning for the unexpected, companies have to weigh the risk versus the cost of creating such a contingency plan. That's a trade-off that Pete Hugdahl, USAA's assistant vice president of security, frequently confronts. "It gets really difficult when the cost factor comes into play," he said. "Are we going to spend \$100,000 to fence in the property? How do we know if it's worth it?"

And—make no mistake—there is no absolute answer. Whether you spend the money or accept the risk is an executive decision, and it should be an informed decision. Half-hearted disaster recovery planning (in light of the BP oil spill of 2010, the 2005 hurricane season, 9/11, the Northeast blackout of 2003, and so on) is a failure to perform due diligence.

This document was compiled from articles published in CSO magazine and CSOonline.com. Contributing writers include Joan Goodchild, Bill Brenner, Scott Berinato, Kate Walsh, Kathleen Carr, Daintry Duffy, Michael Goldberg, and Sarah Scalet.

What else can I do?

Cloud services company [Evolve IP](#) has created a list of suggestions for executives to evaluate their current disaster avoidance plans or, should a plan not exist, provide directional measures to protect their information and communications systems.



CBRNE-TERRORISM NEWSLETTER – November 2017**Establish a disaster recovery functional team**

Elect one spokesperson from the group for communication. In the event of a multi-location organization each location should have a core team or representative that works with the corporate entity.

Risk assessment

Identify risks in the following areas:

Information – What information and information systems are most vital to continue to run the business at an acceptable level?

Communication Infrastructure – What communications (email, toll free lines, call centers, VPNs, Terminal Services) are most vital to continue to run the business at an acceptable level?

Access and Authorization – Who needs to access the above systems and in what secure manner (VPN, SSL, DR Site) in the event of a disaster?

Physical Work Environment – What is necessary to conduct business in an emergency should the affected location not be available?

Internal and External Communication – Who do we need to contact in the event of an emergency and with what information?

Cloud-based data centers and applications

Create a written recovery plan that is hosted remotely in a secure and redundant data center. Schedule and test your plan at least once per year or in accordance with regulatory/compliance requirements. Ensure employees can access the hosted environment (both from within the business confines and remotely) during fail-over mode from the designated locations.

Derek Slater helped create and launch CSO in 2002, and served as Editor in Chief of the magazine and website from 2006 through 2013.

Disaster recovery vs. security recovery plans: Why you need separate strategies

By John Edwards

Source: <https://www.csoonline.com/article/3218083/disaster-recovery/disaster-recovery-vs-security-recovery-plans-why-you-need-separate-strategies.html>

Many enterprises blend their disaster recovery and security recovery plans into a single, neat, easy-to-sip package. But does this approach make sense?

Not really, say a variety of disaster and security recovery experts, including Marko Bourne, who leads Booz Allen's emergency management, disaster assistance and mission assurance practice. "Security and disaster plans are related, but not always the same thing," he observes.

[Read our review of [4 top disaster recovery packages](#). | Get the latest from CSO by [signing up for our newsletters](#).]

The objectives in disaster recovery and security recovery plans are inherently different and, at times, conflicting, explains Inigo Merino, former senior vice president of Deutsche Bank's corporate security and business continuity unit and currently CEO of cyber threat detection firm Cienaga Systems. "The most obvious difference is that disaster recovery is about business continuity, whereas information security is about information asset protection," he notes. "The less evident aspect is that security incident response often requires detailed root cause analysis, evidence collection, preservation and a coordinated and--often--stealthy response."

Such operations usually have to be handled very delicately. "On the other hand, [business continuity plans] are by nature very public events, requiring all hands on deck, large scale communications with the objective of rapid, tactical business resumption," says Merino.

For disaster recovery plans, you almost focus on data quality first and then business processing second," says Scott Carlson, a technical fellow at BeyondTrust, an identity management and vulnerability management products developer. "For security, you rely on capability of protective control with less regard for whether or not you lost past data-- it's much more important to 'protect forward' in a security plan."



Similar, yet different

Many enterprises combine their disaster and security strategies as a matter of convenience, lured by the plans' apparent superficial similarities. "At a high-level, disaster recovery and security plans both do similar activities," says Stieven Weidner, a senior manager with management consulting firm Navigate. "Initially, both plans will have procedures to minimize the impact of an event, followed closely by procedures to recover from the event and, finally, procedures to test and return to production," he notes. Both types of plans also generally include a "lessons learned" process to minimize the possibility of a similar event occurring again.

Yet scratching the surface reveals that disaster and security recovery plans are actually fundamentally different. "[Disaster] recovery plans are focused on recovering IT operations, whereas security plans are focused on preventing or limiting IT interruptions and maintaining IT operations," Weidner notes.

A security recovery plan is designed to stop, learn, and then correct the incident. "A disaster recovery plan may follow similar steps, but nomenclature would not likely use 'detection' to describe a fire or flood event, nor would there be much in the way of analytics," says Peter Fortunato, a manager in the risk and business advisory practice at New England-based accounting firm Baker Newman Noyes. "Further, not many disasters require the collection of evidence."

Another risk in merging plans is the possibility of gaining unwanted public attention. "For instance, invoking a disaster recovery plan often requires large-scale notifications going out to key stakeholders," Merino says. "However, this is the last thing you want during an issue requiring investigation, such as a suspected [network] breach, because of the need to collect and preserve the integrity of highly volatile electronic evidence."

Stitching together complex security and disaster recovery rules and procedures can also result in the creation of a needlessly bulky, ambiguous and sometimes contradictory document. "If you try to combine processes and resources into a single plan, it can muddy the waters, oversimplifying or overcomplicating the process," states Dan Didier, vice president of services for GreyCastle Security, a cybersecurity services provider. While some disaster and security recovery processes may be similar, such as ranking an incident's overall impact, other processes are not as easy to combine. "In addition, you are likely to have different resources involved, so training and testing is complicated, as are updates to the plan after the fact," Didier explains.

Fires, storms, blackouts and other physical events are all unpredictable, yet their nature is generally well understood. Security threats, on the other hand, are both unpredictable and, given the rapidly advancing nature of cyber criminality, not generally well understood, either. This means that security recovery strategies must be revisited and updated more frequently than their disaster recovery counterparts.

A security recovery plan is undoubtedly more difficult to keep up-to-date than a disaster recovery plan, says Anthony McFarland, a privacy and data security attorney in the Nashville office of the law firm Bass, Berry and Sims. "New external cyber threats arise weekly," he notes. The list of man-made or natural disasters that could threaten a business, however, is relatively static. "Even when a business expands geographically, the number of new anticipatable disasters is limited, McFarland says.

Response to a disaster must be immediate, yet response to a cyber-event must be even quicker. "This response reality is amplified because a company may have forewarning of a pending disaster, like a tornado, flood or earthquake, but no advance notice of a targeted cyberattack," McFarland says.

"The nature of the threats within security recovery plans are more dynamic than within disaster recovery, and therefore require continual review and update," says Mark Testoni, president and CEO of SAP National Security Services. "For example, recent ransomware attacks, such as WannaCry, are incredibly destructive and require security recovery plans to examine how to effectively respond to new threats and risks."

The discovery process is the most important aspect of both security and disaster planning, Bourne says. "Plans must be adaptable and key leaders must understand what the plans are trying to achieve in order to ensure maximum success," he adds.

Making it a team effort

While most experts advocate creating and maintaining separate disaster and security recovery plans, they also note that both strategies must be periodically examined for potential gaps and conflicts. "The best course of action to have the plans complement one another is to make sure that you have the same team working through both of them," says



CBRNE-TERRORISM NEWSLETTER – November 2017

Steve Rubin, a partner at the Long Island, N.Y., law firm Moritt Hock & Hamroff, and co-chair of its cybersecurity practice group. "Not only will they will be stronger and complement one another, but will also be more effective and resilient in the long run."

	Disaster recovery plan	Security recovery plan
Primary objective	Provide business continuity after disruption from man-made or natural causes	Protect data assets after a data breach
Response requirements	Open communication with stakeholders, focus on rapid data recovery	A stealthy approach that includes evidence collection and preservation, and root cause analysis
Tactical differences	Rapid, accurate data recovery	Protective controls focused on preventing future loss
Plan management	Dedicated team that focuses on best practices and lessons learned from disaster recovery experiences	Dedicated team that keeps up to date on new cyber security threats and modifies the plan accordingly

CSO

Weidner notes that it's okay, however, to have separate teams in charge of security and disaster plans as long as they regularly coordinate their strategies and goals with each other. "Each team, whether supporting security or IT recovery, needs to manage their own specific plan requirements," Weidner says. "However, oversight and governance should be centralized to guarantee events will be supported using the same methodology, such as communications to executive teams, company stakeholders and customers."

Whether planning is handled by one or two teams, the right people need to be brought onboard, Didier says. "Senior management plays a critical role and must oversee the operation," he says.

"The CIO, CISO and network administrators will be integral members of both teams," McFarland observes. However, many disaster recovery team members will have no, or only limited, involvement in the work of the security group, and vice-versa. "For example," McFarland notes, "facilities managers are critical members of a disaster recovery team, but typically not needed in the [security] group unless there was a physical loss or theft of tangible/hardcopy data from an office."

Operations and security teams should review each other's plans in a controlled and constructive manner to determine how they can be leveraged in support of each other, suggests Morey Haber, vice president of technology at BeyondTrust. "These policies should not be developed on islands and if possible be tested together," he says. "This helps address extreme edge cases while maintaining separation of duty requirements and building team synergies."

Lessons learned

As enterprises learn what works and what doesn't work in both security and disaster recovery planning, a growing number now realize that security recovery is not disaster recovery and that each has very different needs. "As organizations mature, they learn that the purpose of security incident response is much more nuanced than merely a restoration of business and that many of the functions typically invoked in disaster recovery for business continuity purposes are either not applicable to cyber security events, or in some cases, harmful to security incident response and forensics," Merino says.

"The key to having successful security and disaster recovery plans is to document, manage, test plans and and develop a common governance, communication and escalation methodology," Weidner says. "This unified approach will minimize confusion and decrease the time to recover from events."

