

December 2015

CBRNE NEWSLETTER TERRORISM

E-Journal for CBRNE & CT First Responders



**PART
B**

www.cbrne-terrorism-newsletter.com

RBS under fire for investing in weapons of mass destruction

Source: http://www.heraldscotland.com/news/14095352.RBS_under_fire_for_investing_in_weapons_of_mass_destruction/

The Royal Bank of Scotland (RBS) has been accused of making money from weapons of mass destruction after it was named as the biggest financial backer of nuclear bombs in the UK.

New international analysis by disarmament groups reveals that over the last four years RBS has lent £4.5

billion to 21 major companies involved in nuclear weapons in the UK, the US, France and India. They include firms that work on the Trident weapons systems, such as BAE Systems, Lockheed Martin, Jacobs Engineering and Serco.

One of the bank's most controversial loans has been £27 million to Larsen & Toubro, which develops the launcher system for India's Akash nuclear missiles. India is widely regarded as a nuclear outlaw because it has not signed the nuclear non-proliferation treaty.

'Don't Bank on the Bomb', a report compiled by the Dutch peace organisation Pax and the International Campaign to Abolish Nuclear Weapons (ICAN), lists RBS in a "hall of shame" for its nuclear loans. Other UK banks on the list include Barclays with £3.8bn in loans, HSBC with £2.9bn, Old Mutual with £2.8bn and Lloyds with £1.3bn.

Internationally the report names 382 banks, insurance companies and pension funds from 27 countries that have made £323 billion available to nuclear weapons producers since January 2012. It also highlights the fast-growing number of financial institutions – 53 – that now prohibit or limit their nuclear investments.

One of the report's authors, Wilbert van der Zeijden from Pax, was in Scotland last week briefing politicians and campaigners on his findings. Most Scottish people, most Scottish political parties and the Church of Scotland have all rejected Trident, he pointed out.

"It's time the biggest Scottish bank, RBS, stopped financing the companies making Trident," he said. "While Scotland is trying to get rid of weapons of mass destruction, RBS is trying to make money on them."

RBS did have a policy of restricting its loans to weapons companies, but this had not prevented it from financing 21 nuclear weapons companies, Zeijden added. "A treaty banning nuclear weapons is coming. Continuing to invest in their producers is a bad investment strategy."

Rebecca Sharkey, coordinator ICAN UK, said: "Anyone with a Royal Bank of Scotland bank account or pension may be unwittingly and unwillingly complicit in funding companies that produce weapons of mass destruction."

The new report would increase the financial stigma on nuclear weapons, she argued. "It will help people and institutions to divest ahead of a new global ban treaty that will likely make the financing of nuclear weapons illegal as part of a wider prohibition."

John Ainslie, coordinator of the Scottish Campaign for Nuclear Disarmament, pointed out that in the Netherlands banks had been forced to rethink their investments in nuclear weapons after customers threatened to take their business elsewhere.

"Just when you thought the reputation of RBS couldn't fall any lower, we find out that they are taking our money and investing it in nuclear weapons," he said. "RBS don't just support Trident they also fuel proliferation by funding India's nuclear missile program."

RBS was bailed out by the UK government after the financial crisis in 2008 and is now 73 per cent publicly owned. In recent years the bank has been refocusing its business to become simpler and more concentrated on the UK.

An RBS spokesman did not dispute the loans to nuclear bomb companies. "All of our lending to defence companies is subject to enhanced due diligence," he said.

"RBS operates a clear prohibition on the funding of highly controversial weapons including cluster munitions, anti-personnel landmines, biological and toxin weapons, chemical weapons and blinding laser weapons."



Israel has **115** nuclear warheads: Report

Source: <http://www.middleeasteye.net/news/report-israel-has-115-nuclear-warheads-1915845762#sthash.X9hdZcDM.dpuf>



A picture taken on 8 March 2014 shows a partial view of the Dimona nuclear power plant in the southern Israeli Negev desert (AFP)

Nov 22 – **A new US report** says that Israel possesses 115 nuclear warheads in its secret arsenal of weapons of mass destruction.

The report by the Washington DC-based Institute for Science and International Security (ISIS), indicates that the arsenal is larger than previously thought, with most previous estimates suggesting Israel had around **80 warheads**, which brought it roughly on par with the nuclear capabilities of India and Pakistan. Other estimates have put the figure much higher, at closer to 200, highlighting the secrecy that continues to shroud Israel's nuclear programme.

The ISIS report, which was based on previous reports and investigations, also states that Israel has produced about 660 kilograms of plutonium at the Dimona reactor in the Negev desert.

Israel's Military Stock of Plutonium, end of 2014	
Military Plutonium	660 ± 115 kg

The site includes a heavy water reactor, a fuel fabrication plant and a plutonium separation plant, all of

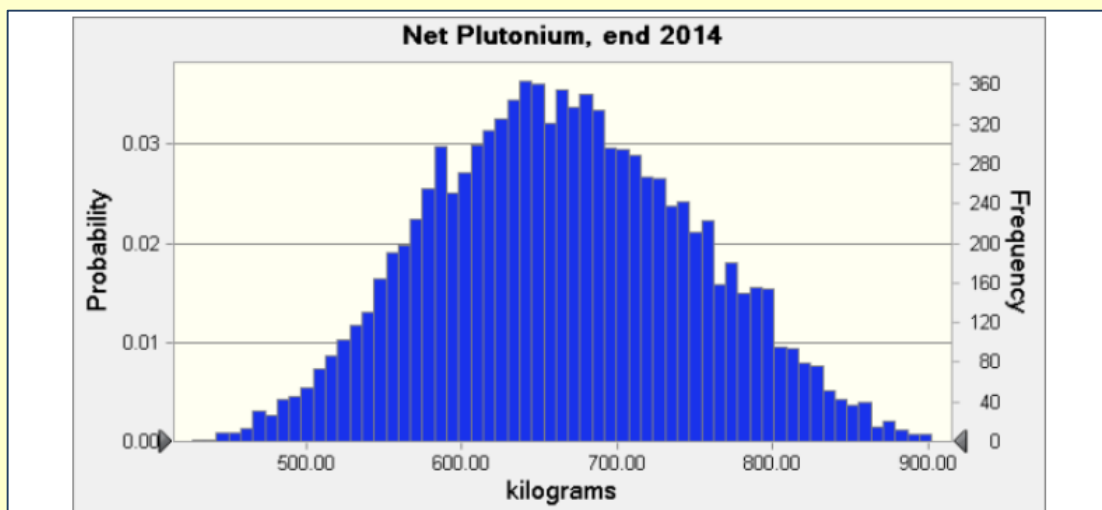
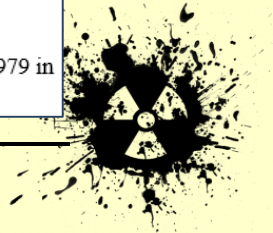


Figure 1: Total plutonium, reflecting small drawdowns due to processing losses and possibly nuclear test in 1979 in South Atlantic.



CBRNE-TERRORISM NEWSLETTER – December 2015

which were secretly provided by France in the 1950s and early 1960s.

The US, France, Germany, Britain and even Norway are also widely believed to have supplied Israel with nuclear materials at the time, allowing it to build up a clandestine and as yet never officially declared nuclear arsenal, neither confirming nor denying its stockpiles.

According to the report, which was published by the institute on its website on Thursday, each nuclear warhead carries between 3-5 kilograms of plutonium. The report revealed that Israel began to develop its nuclear programme in 1963.

While many have long known about the programme, its existence was confirmed by the declassification of formerly secret US government documents, with its existence further revealed by former Israeli nuclear technician Mordechai Vanunu, who in 1986 said that the nuclear weapons programme was much larger than commonly assessed at that time.

Israel was the sixth country in possession of nuclear weapons, after the five permanent members of the UN Security Council.

The Doomsday Scam

By C. J. Chivers

Source: <http://www.nytimes.com/2015/11/22/magazine/the-doomsday-scam.html?ref=topics>



Nov 19 – The hunt for the ultimate weapon began in January 2014, when Abu Omar, a smuggler who fills shopping lists for the Islamic State, met a jihadist commander in Tal Abyad, a Syrian town near the Turkish border. The Islamic State had raised its black flag over Tal Abyad several days before, and the commander, a former cigarette vendor known as Timsah, Arabic for “crocodile,” was the area’s new security chief. The Crocodile had an order to place, which he said he had received from his bosses in Mosul, a city in northwestern Iraq that the Islamic State would later overrun.

Abu Omar, a Syrian whose wispy beard hinted at his jihadist sympathies, was young, wiry and adaptive. Since war erupted in Syria in 2011, he had taken many noms de guerre — including Abu Omar — and found a niche for himself as a freelance informant and trader for hire in the extremist underground. By the time

he met the Crocodile, he said, he had become a valuable link in the Islamic State’s local supply chain. Working from Sanliurfa, a Turkish city north of the group’s operational hub in Raqqa, Syria, he purchased and delivered many of the common items the martial statelet required: flak jackets, walkie-talkies, mobile phones, medical instruments, satellite antennas, SIM cards and the like. Once, he said, he rounded up 1,500 silver rings with flat faces upon which the world’s most prominent terrorist organization could stamp its logo. Another time, a French jihadist hired him to find a Turkish domestic cat; Syrian cats, it seemed, were not the friendly sort.

War materiel or fancy; business was business. The Islamic State had needs, it paid to have them met and moving goods across the border was not especially risky. The smugglers used the same well-established routes by which they had helped foreign



CBRNE-TERRORISM NEWSLETTER – December 2015

fighters reach Syria for at least three years. Turkish border authorities did not have to be eluded, Abu Omar said. They had been co-opted. “It is easy,” he boasted. “We bought the soldiers.”

This time, however, the Crocodile had an unusual request: The Islamic State, he said, was shopping for red mercury.

Abu Omar knew what this meant. Red mercury — precious and rare, exceptionally dangerous



and exorbitantly expensive, its properties unmatched by any compound known to science — was the stuff of doomsday daydreams. According to well-traveled tales of its potency, when detonated in combination with conventional high explosives, red mercury could create the city-flattening blast of a nuclear bomb. In another application, a famous nuclear scientist once suggested it could be used as a component in a neutron bomb small enough to fit in a sandwich-size paper bag.

Abu Omar understood the implications. The Islamic State was seeking a weapon that could do more than strike fear in its enemies. It sought a weapon that could kill its enemies wholesale, instantly changing the character of the war. Imagine a mushroom cloud rising over the fronts of Syria and Iraq. Imagine the jihadists’ foes scattered and ruined, the caliphate expanding and secure.

Abu Omar thought he might have a lead. He had a cousin in Syria who told him about red mercury that other jihadists had seized from a corrupt rebel group. Maybe he could arrange a sale. And so soon Abu Omar set out, off for the front lines outside Latakia, a Syrian

government stronghold, in pursuit of the gullible man’s shortcut to a nuclear bomb.

To approach the subject of red mercury is to journey into a comic-book universe, a zone where the stubborn facts of science give way to unverifiable claims, fantasy and outright magic, and where villains pursuing the dark promise of a mysterious weapon could be rushing headlong to the end of the world. This is all the more remarkable given the broad agreement among nonproliferation specialists that red mercury, at least as a chemical compound with explosive pop, does not exist.

Legends of red mercury’s powers began circulating by late in the Cold War. But their breakout period came after the Soviet Union’s demise, when disarray and penury settled over the Kremlin’s arms programs. As declining security fueled worries of illicit trafficking, red mercury embedded itself in the lexicon of the freewheeling black-market arms bazaar. Aided by credulous news reports, it became an arms trafficker’s marvelous elixir, a substance that could do almost anything a shady client might need: guide missiles, shield objects from radar, equip a rogue underdog state or terrorist group with weapons rivaling those of a superpower. It was priced accordingly, at hundreds of thousands of dollars a kilogram. With time, the asking price would soar.

As often happens with durable urban legends, the red-mercury meme found just enough public support to assure an unextinguishable life. Chief among its proponents was Samuel T. Cohen, the American physicist and Manhattan Project veteran often called the father of the neutron bomb, who before his death in 2010 spoke vividly of the perils of nuclear terrorism and what he said was poor government preparation for such attacks. Cohen joined the red-mercury bandwagon as it gathered momentum in the early 1990s, staking a lonely position by asserting that the substance could be used to build nuclear weapons of exceptionally small size.

In one edition of his autobiography, he claimed red mercury was manufactured by “mixing special nuclear materials in very small amounts into the ordinary compound and then inserting the mixture into a nuclear reactor or bombarding it with a particle-accelerator beam.” The result, he said, “is a remarkable nonexploding high explosive” that, when detonated, becomes “extremely hot, which allows pressures and



CBRNE-TERRORISM NEWSLETTER – December 2015

temperatures to be built up that are capable of igniting the heavy hydrogen and producing a pure-fusion mini neutron bomb.” Here was a proliferation threat of an order never before seen.

The establishment largely dismissed him. “If he did ever reveal evidence, I never saw it,” said Peter D. Zimmerman, a nuclear physicist who served as chief scientific adviser for the U.S. Arms Control and Disarmament Agency at the time. He added, “I would have seen it, at that point in history.” Jeffrey Lewis, a nonproliferation analyst at the James Martin Center for Nonproliferation Studies in Monterey, Calif., put matters less delicately, saying Cohen followed a classic formula for conspiracy theories, mixing “nonscientific mumbo jumbo” with allegations that governments were withholding the truth. “I could never figure out where Sam Cohen the physicist ended and Sam Cohen the polemicist began,” he said.

Outside this circle of the faithful, red mercury faced doubters. The substance was almost everything but scientifically verifiable. It was not even reasonably explicable. “Over all it doesn’t make much sense,” an engineer at Los Alamos National Laboratory wrote to a supervisor in 1994. It was also devilishly elusive, turning up in tales of smuggling mafias but never quite finding its way to a law-enforcement body or nuclear agency for proper frisking. When hopeful sellers were caught, substance in hand, it reliably turned out to be something else, sometimes a placebo of chuckle-worthy simplicity: ordinary mercury mixed with dye. The shadowy weaponeer’s little helper, it was the unobtainium of the post-Soviet world. Among specialists who investigated the claims, the doubts hardened to an unequivocal verdict: Red mercury was a lure, the central prop of a confidence game designed to fleece ignorant buyers. “Take a bogus material, give it an enigmatic name, exaggerate its physical



Russian news organizations in the 1990s nevertheless relayed claims of red mercury’s destructive potential at face value, and foreign news outlets occasionally repeated them, boosting the material’s credibility and mystique. Britain’s Channel 4 elevated the material’s profile with two documentaries — “Trail of Red Mercury” and “Pocket Neutron” — that presented, according to their producers, “startling evidence that Russian scientists have designed a miniature neutron bomb using a mysterious compound called red mercury.” Cohen held a news conference after one broadcast to say it confirmed his fears.

properties and intended uses, mix in some human greed and intrigue, and *voilà*: one half-baked scam,” the Department of Energy’s Critical Technologies Newsletter declared. In 1998, 15 authors from the Lawrence Livermore National Laboratory, which helps maintain the American nuclear-weapons stockpile, published an article in *The Journal of Radioanalytical and Nuclear Chemistry* that called red mercury “a relatively notorious nuclear hoax.” In 1999, *Jane’s Intelligence Review* suggested that the scam’s victims may have included Osama bin Laden, whose Qaeda purchasing



CBRNE-TERRORISM NEWSLETTER – December 2015

agents were “nuclear novices.” The most accommodating theory held that red mercury might have been a Soviet code name for something else — maybe lithium-6, a controlled material with an actual use in nuclear weapons — and traffickers repurposed the label for whatever nuclear detritus they were trying to move.

A true believer of the legends might interject that official skepticism in public did not preclude another discussion playing out on classified channels. But when WikiLeaks published American diplomatic cables in 2010 and 2011, snippets of the internal red-mercury dialogue were consistent with the public statements. In 2006, according to one cable, Sri Lanka notified the American Embassy in Colombo of concerns that the Tamil Tigers, a secessionist militant group, had tried to procure the substance. “Red Mercury is a well-known scam material,” a State Department nonproliferation official told the embassy. “There is nothing to be concerned about.”

Few people are more familiar with the lingering red-mercury assertions than Zimmerman, who later became director of the Center for Science and Security Studies at King’s College in London. For years, he canvassed his peers in nuclear-weapons and nonproliferation communities. He asked about the substance in conferences. He brought it up in one-on-one sessions with weaponeers from multiple countries and scientists from the former Communist bloc. He concluded that the substance was not just “hot air, myth, smoke and mirrors” but also “a con job.”

When I called him, he laughed and referred to people convinced of its powers as “Red Mercurians.” Some of the stories he’d heard, he said, resembled “an old Jack Benny routine.” He paused to be straightforward and clear. Red mercury (or, for that matter, any mercury compound of any color), he said, had no nuclear-weapons application of any sort. The particulars of its supposed martial utility do not square with basic science. “It cannot be true,” he said, and spoke as if restating a longstanding challenge. “I have plenty of times staked my reputation on these statements, and no one has ever called me on it.”

And yet a generation after the hype first burned bright, shopworn legends of red mercury’s powers, lodged in fringe provinces of the popular imagination, continue to surface, rekindled by shifting casts of jihadists, tomb

looters, smugglers, journalists, YouTube salesmen and other wannabe profiteers. One thing about red mercury: If it’s not nuclear, it’s viral.

Abu Omar had joined a long line of players. It was impossible not to wonder: Did he really believe in red mercury himself?

When the Crocodile placed his order, Abu Omar said, the smuggler asked how much the Islamic State was willing to pay. The answer was vague. The Islamic State would pay, he said, “whatever was asked.” This was not the practical guidance a businessman needs. So the Crocodile sharpened the answer. Up to \$4 million — and a \$100,000 bonus — for each unit of red mercury matching that shown in a set of photographs he sent to Abu Omar over WhatsApp, the mobile-messaging service.

The images showed a pale, oblong object, roughly the length of a hot-dog bun, with a hole at each end. It bore no similarity to the red mercury that smugglers often described — a thick liquid with a brilliant metallic sheen. It appeared to be a dull piece of injection-molded plastic, like a swim-lane buoy or a children’s toy. But it had an intriguing resemblance that hinted at how the Islamic State’s interest might have been piqued: It was the exact likeness of an object that in 2013 the Cihan News Agency, one of Turkey’s largest news agencies, had called a red-mercury rocket warhead.

In that case, three men were said to have been arrested near Kayseri, a city in central Turkey. Cihan’s coverage followed the familiar arc of red-mercury hype. Footage shot at night showed officials in protective suits and masks approaching a van. The news presenter reported the operation in matter-of-fact tones, noting that the seized rocket component “was examined by six different institutions, including the Turkish Atomic Energy Authority, all of which found that it contained the material red mercury. The liquid can cause large explosions and is worth \$1 million per liter. Red mercury is used for intercontinental rocket systems and hydrogen bombs.”

With that validation, the photographs traveled on social media, finding their way to the Islamic State and then to Abu Omar, who said he remembered something he had heard from his cousin in Syria, a fighter for Jabhat al-Nusra, the Qaeda affiliate and bitter Islamic State rival. This cousin, he said, had told him that Nusra fighters had taken red-mercury warheads from a now-defunct rebel



CBRNE-TERRORISM NEWSLETTER – December 2015

group, Ghuraba al-Sham, which the jihadists had overpowered in 2013, executing its leaders. The warheads that the Nusra fighters confiscated, Abu Omar said, matched those in the Crocodile's photographs.

Not long after leaving Tal Abyad, Abu Omar said, he tracked down his cousin near the front lines outside Latakia to arrange a sale. The plan quickly tanked. His cousin, he said, suspected Abu Omar was shopping for the Islamic State. He refused to discuss terms. "I want you to end this talk about red mercury because I know where it is going to go," Abu Omar recalled his cousin saying. "I know ISIS wants them. But we will never sell."

Abu Omar was describing all this in the lobby of a Turkish hotel, where he appeared one night this fall after several phone calls and chat sessions. His stories were more than far-fetched; they were confounding. Anyone with an Internet connection could quickly discover that the red-mercury meme was widely regarded as nonsense. Even a visit to Wikipedia — whose entry on the subject began, "Red mercury is a hoax substance of uncertain composition" — would surely be enough to raise questions for anyone disbursing Islamic State cash. I told Abu Omar that I had spoken with several nonproliferation experts, and they roundly agreed: Red mercury was a scam. Did he believe otherwise?

Abu Omar listened patiently. His face gave nothing away. Then he replied politely, as if addressing the uninformed. "I have seen it with my own eyes," he said.

Two years before in Ras al-Ain, another Syrian border town, Abu Omar said, he was with a group of Islamic fighters that organized a test with 3.5 grams of liquid red mercury and a container of chlorine. The experiment was led by Abu Suleiman al-Kurdi, who commanded a small fighting group that has since joined the Islamic State. Al-Kurdi gathered the jihadists around his materials as the test began. "I will count to 10, and whoever stays in the room after that suffocates and dies," he warned.

The chlorine was held in a foil-lined container, Abu Omar said. As the group watched, al-Kurdi dipped a needle into the red mercury and then touched the needle to the chlorine, transferring a drop. "Everything interacted with everything," Abu Omar said, and a foul vapor rose. All of the fighters were driven away, first from the room, then from the house.

The powers of red mercury, Abu Omar said, were real.

Almost every aspect of this story, like so many other breathless accounts of red mercury, was unverifiable. And even if something did happen in that room, the noxious vapors could have a simple explanation: Chlorine alone damages the respiratory tract and can be deadly if inhaled.

Safi al-Safi, an unaffiliated rebel and small-time smuggler specializing in weapons, antiques and forged documents, sat in an open-air cafe beside the Syrian-Turkish border. He was smoking scented tobacco from a water pipe while discussing the cross-border mercury trade. "Red mercury has a red color, and there is mercury that has the color of dark blood," he said. "And there is green mercury, which is used for sexual enhancement, and silver mercury is used for medical purposes. The most expensive type is called Blood of the Slaves, which is the darkest type. Magicians use it to summon jinni."

This primer — passionate, thorough, outlandish to its core — fits a type. In meetings with smugglers in several towns along the border, red mercury inhabited the fertile mental terrain where fear and distrust of authority meet superstitious folklore. Descriptions of the material varied slightly in detail and sharply in price, and there were ample contradictions. But there was a remarkable consistency in several intricate legends and origin stories, even among people who did not know one another and who were separated by many miles.

Another smuggler, Faysal, who said he was awaiting results of vetting by the United States government to join a Pentagon-backed force opposing the Islamic State (the program has since been dropped), continued the lesson. "It has two different types: hot and cold," he said. The cold form, which other smugglers sometimes call "spiritual mercury," he said, "can be found in Roman graveyards." He added: "Kings and princes and sultans used to take it to the graves with them."

This type of red mercury, the smugglers said, has been recovered by Middle Eastern grave robbers for at least several decades. "In previous generations, old women wore it in a necklace to keep the devil's eye away," Faysal said. More recently, rich men shopped for cold red mercury as either an aphrodisiac or to improve their sexual performance.



CBRNE-TERRORISM NEWSLETTER – December 2015

The substance was so valuable that dishonest traders, al-Safi said, often trafficked in fake red mercury. “In my village at least 15 people trade in it,” he said. “They buy normal mercury, and they color it. They use red lipstick and put a little on a spoon and heat the spoon until it turns to powder, and you put the powder in the mercury, and you mix it, and it becomes that color. This is how you cheat it.”

Identifying such cheats was easy, the smugglers said, because real red mercury is attracted to gold but repelled by garlic. Wise buyers bring gold and garlic to test the product before cash changes hands. “You put a drop on a plate and you approach it with garlic, and that drop is going to move away,” a third smuggler, Abu Zaid explained. “But if you put red mercury on a plate and move a piece of gold under the plate, the red mercury is going to move with it.”

Cold red mercury, these smugglers said, could not be used for nuclear weapons; that was the role of hot red mercury, which had a more recent origin. Only sophisticated laboratories manufactured it, and the hot red mercury available in Syria had come from the Soviet Union — usually, according to Raed, another smuggler, “in a specially maintained box with equipment and a manual and special gloves.”

Abu Zaid said hot red mercury was sometimes offered for sale in Syria and could be useful for the Islamic State, which has a cadre of former Iraqi officials who would know how to harness its power. But he cautioned that buyers could easily make a grievous mistake. “It is not only about getting the red mercury,” he said. “The very small box needs special equipment to open it, and special reactors to work with it. If you open this box, a radius of eight kilometers around you will be destroyed.”

This was especially dangerous, because hot red mercury could also be harvested from junkyards and seamstress shops. Al-Safi described how this came to pass. To prevent the weapons-grade material from falling into the wrong hands during what he called “the American occupation” of the former Soviet Union, he said, Russians safeguarding the stock late in the Cold War cached tiny reservoirs of red mercury in sewing machines and radios bound for export, which were then scattered throughout the Arab world. (Another version of the same tale says that red mercury is hidden in old television sets.)

These rumors have been circulating for years, once driving prices for old sewing machines as high as \$50,000 in Saudi Arabia, according to a 2009 Reuters report. Often the most-sought-after machines were the Singer brand — which, considering that Singer was an American manufacturer, did not quite align with the Soviet fable. No matter. Abu Omar also insisted that old sewing machines were a red-mercury source. “Specific machines,” he said, “with a butterfly logo on them.” He said he knew this from experience because the red mercury used in the jihadists’ chlorine experiment in Ras al-Ain had come from his grandmother’s machine.

If all of this seems like a bad and ever-expanding joke, it can work that way. When I mentioned the garlic-and-gold tests and red mercury’s supposed qualities as a sexual stimulant to Peter Zimmerman, the nuclear physicist, his answer came quickly. “Take that with a grain of red mercury,” he said.

Jokes may be as useful a means as any of understanding red mercury, considering another origin theory that has made the rounds for years: that the hoax has roots in an intelligence-service put-on, a disinformation campaign of phony news articles planted decades ago in Russian newspapers by the K.G.B. and one of its successors, the F.S.B.

There are other variants of this story, including one in which Washington and Moscow collaborated in circulating red-mercury stories to flush out nuclear smugglers and to waste terrorists’ time. American soldiers and officers in bomb-disposal and counter-W.M.D. jobs shared that version with me, although, once again, no one had evidence for its veracity. It was something that they had heard on their jobs and a story they admitted that they liked — the thinking being that if the Four Lions wanted to shop for photon torpedoes, let them shop; that would be preferable to how the Islamic State otherwise spends its time. (Abu Omar, for example, said the Islamic State had also sought his help in abducting Western journalists.)

And yet the U.S. military and its allies, too, had found themselves expending resources on the hoax. In early 2011, a European military unit in Afghanistan handed over supposed red mercury to their American colleagues at Task Force Paladin, the command charged with countering and analyzing improvised bombs. The handoff



CBRNE-TERRORISM NEWSLETTER – December 2015

triggered an international counterproliferation response, according to several American soldiers familiar with the events and an officer who participated in the operation but requested anonymity because parts of it remain classified. Task Force Paladin alerted the 20th Chemical, Biological, Radiological, Nuclear, Explosives Command, the primary U.S. Army unit trained to eliminate threats of W.M.D., that they had an unknown substance that could be dangerous material. Back at the command's headquarters in Maryland, teams of specialists in nuclear disablement and chemical response were packed into a C-5 military-transport jet and rushed to Bagram Air Base, where they were shown two small, lead-lined containers. One was about the dimensions of a quart-size Mason jar; the other roughly the size of a pint glass.

The nuclear-disablement team went first but found no sign that the containers held anything radioactive. They then passed the job to the chemical-warfare specialists and bomb-disposal techs. External tests on the containers were inconclusive, the officer involved said, so the soldiers took up the unenviable task of breaching the vessels to find out what exactly was inside. Wearing protective suits and breathing apparatuses, they put the first lead-lined container inside an airtight glove box within what the officer called a "secure, reinforced" shipping container, and then monitored it from afar by video as the spinning bit from a remote-controlled power drill plunged through the container's soft wall. Out spilled ordinary mercury, the old standby of red-mercury scams. The second container was empty. In all, the officer said, the mercury amounted to "about a quarter or half cup."

The American soldiers quietly packed up and flew home. Their mission is memorialized in the Army's classified records with a title — Operation Chimera — that members of the American bomb-disposal community said suggested a certain sense of humor about the whole affair. How the Europeans had been deceived is not publicly known. (One American familiar with the events said a European special-forces team had been lured into a bad buy.) On that matter, the American military declined to comment.

This was hardly the worst of the hoax's real-world effects. In southern Africa, it has cost lives. According to a regional and especially cruel variation of the legend, the substance is

found in conventional military munitions, particularly land mines, there to be claimed by anyone daring enough to take them apart and extract the goods. Tom Dibb, the program manager in Zimbabwe for the Halo Trust, a private mine-clearing organization, said he and the local authorities have documented people being killed in explosions while hunched over land mines or mortar bombs with hand tools.

In the bloodiest incident, in 2013, six people were killed near Harare, Zimbabwe's capital, by a blast in the home of a faith healer. One victim was an infant. Dibb spoke with the police and said "they were pretty convinced that it was a tank mine being taken apart for red mercury." In another case, which Dibb examined himself, two men were killed and another wounded as they tried harvesting land mines for red-mercury extraction from a minefield. The most recent death that the Halo Trust investigated occurred on Nov. 1, Dibb said, when a 22-year-old man, Godknows Katchekwama, was killed while trying to dismantle and remove red mercury from an R2M2, a South African antipersonnel land mine about the size of a tuna can.

The explosion outside Harare prompted Michael P. Moore, who manages the Landmines in Africa website, to start a second site, the [Campaign Against Red Mercury](#), which documents hoaxes and urges people not to believe them. Moore said he tried tracing how the meme leapt from sewing machines to explosive devices but could not figure it out. Public-education campaigns were needed, he said, because "it's enough of a pervasive myth that it's not going to go away anytime soon. And people are dying."

The Crocodile kept inquiring about red mercury for more than a year, Abu Omar said, pressing for results. He reached out one last time on WhatsApp in June 2015. At the time, Kurds were attacking the Islamic State in Tal Abyad, and the commander also sought what he called "thermal panels" to deceive the weapons-guidance systems on American warplanes. But by November of this year, Abu Omar was still empty-handed. By then Tal Abyad had fallen to the Kurds, and the Crocodile had gone silent, leaving the quest without a sponsor for now.

Abu Omar had kept busy with other work; he said he had recently delivered 23 commercial drones to the jihadists. He remained a storehouse of red-mercury yarns. Word was that the Kurdish fighting



CBRNE-TERRORISM NEWSLETTER – December 2015

groups opposing the Islamic State had been buying up the stuff. “People I know sold it to Kurds three times,” he said. And eight red-mercury warheads had been found in the Aleppo countryside, too. The story was similar to one from Reyhanli, another Turkish border city, where smugglers insisted that rebels in Idlib had overrun a military checkpoint and captured a few grams of red mercury. This material was said to be available for sale, although no one who said this could arrange to see it. It led to an obvious question: If Syria’s military possessed red-mercury weapons, why hadn’t it used them? Why would an imperiled force with a well-documented disregard for restraint forgo uncorking such a weapon as its garrisons fell?

If red mercury seemed a perfect fit for the particular nature of this brutal, shadowy war — an apocalyptic weapon for a terrorist group driven in part by the belief that we are

approaching the return of the Mahdi, the final defeat of infidels and the end of the world — it was not making itself easy to get. All this, and the police were drawing near. In June, Turkish news agencies reported another red-mercury bust, this time of a pair of Georgians. And Abu Omar said an associate of his had managed to obtain the material, only to be arrested in Ankara before he could unload it. The authorities released him but kept his red mercury, he said, for themselves. “His phone was monitored,” Abu Omar said, and thus the bad turn.

None of this was verifiable, either. The Turkish government declined to answer questions about its red-mercury arrests over the last two years. And his friend? Abu Omar said he had fled to Sweden. He provided a link to the man’s Facebook profile, but the man was not replying to requests. You can’t be too careful in the red-mercury game.

C.J. Chivers is a reporter for The Times.

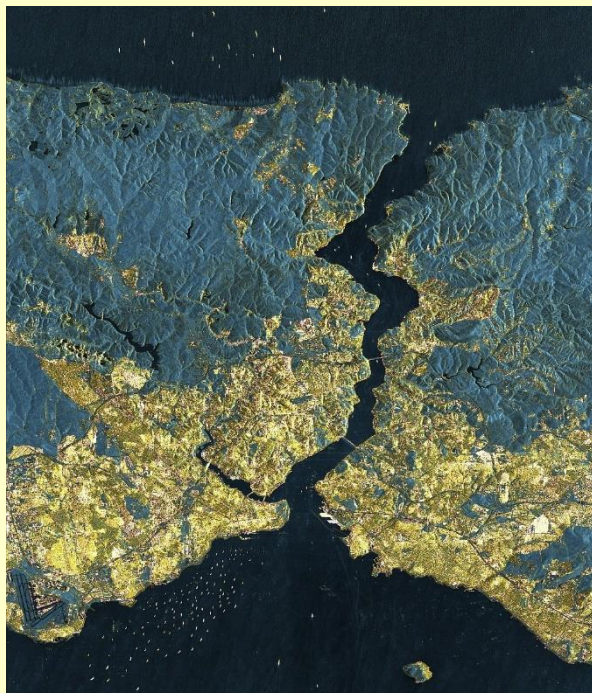
Russia ‘should NUKE enemy number one’ Turkey and wipe out Istanbul

Source: <http://israndjer.blogspot.gr/2015/11/vladimir-zhirinovsky-wants-putin-to.html>

RUSSIA is ready to “use nuclear weapons on enemy number one” Turkey, one of the country’s leading politicians has announced. Political hothead and Russian colonel Vladimir Zhirinovsky called for president Vladimir Putin to wipe out Turkish capital Istanbul, killing nine million people. Turkey’s decision to down a SU-24 fighter jet after it entered their aerospace was branded “stupid” by Zhirinovsky. “A nuclear attack can destroy Istanbul very easily. Just one nuclear bomb in the Istanbul Strait will wash the city away,” he told Moscow Speaking Radio.

DEFIANT: Vladimir Zhirinovsky did not hold his words back when calling for Russia to nuke Turkey—“It would be such a terrible flood, the water would rise to between 10m and 15m and the city would [flood].” “And then there are nine million lives.” The Liberal Democratic Party of Russia leader also called Turkey “enemy number one”. Zhirinovsky’s chilling words come as Turkish president Recep Erdogan warned Putin not to “play with fire”. Fears are now growing the world is on the cusp on another world war.

APOLOGY: Vladimir Putin wants Turkish President Erdogan to say sorry for downing jet-The incident which sparked the tensions



CBRNE-TERRORISM NEWSLETTER – December 2015

DOWNED: The Russian jet was shot down over Syria-Erdogan said he wanted to meet Putin to resolve the ongoing war of words. But Putin wants an apology from Turkey before he will enter talks. He said it was “impossible” for Turkey not to have known it was shooting at a Russian plane. “It’s got an insignia, you can see that very clearly,” Putin added.

Level-2 incident at Bordeaux University: discovery of radioactive sources and incidental exposure of persons

Source: <http://www.french-nuclear-safety.fr/Information/News-releases/Bordeaux-University-discovery-of-radioactive-sources-and-incidental-exposure-of-persons>

Oct 10 – On 18 September 2015, Bordeaux University - Carreire Campus - informed ASN of the discovery of two radioactive sources in a room in the INSERM laboratory.



The laboratory in question has not had a license to hold radioactive sources for many years now due to the cessation of its activities involving radioactive sources.

The two radioactive sources were discovered by the Bordeaux University prevention service in a much cluttered and regularly frequented room during a housekeeping operation carried out at the end of June 2015.

As soon as they were discovered, the sources were transferred for safe storage in a room specially intended for that purpose within the university campus.

On 4 September the university's radiation protection service conducted an inspection to determine the radiological characteristics of the retrieved sources. **Risks of irradiation and**

contamination were evidenced around one of the two sources. It is an unidentified source displaying a dose rate of 3.4 mSv/h on contact.

The radiological inspection of the room did not reveal any radioactive contamination.

On the other hand, according to the first received dose estimates, a person working in this room would have received a dose approaching 20 mSv/year and several others would have received a dose slightly higher than the annual regulatory limit set for the general public (1 mSv).

ASN carried out an inspection at Bordeaux University on 1 October 2015 to examine the circumstances of this event (refer to the inspection follow-up letter). Further to this inspection, ASN asked that an action plan be engaged to prevent a similar event occurring again, and that an estimate be made of the effective doses received by all the personnel that could have been exposed to the ionising radiation.

The shortcomings in the radiation protection culture and the dose potentially received by the exposed persons has led ASN to rate this event level 2 on the INES scale, which comprises 8 levels from 0 to 7.

Rock salt serving to store nuclear waste may not be as impermeable as previously thought

Source: <http://www.homelandsecuritynewswire.com/dr20151130-rock-salt-serving-to-store-nuclear-waste-may-not-be-as-impermeable-as-previously-thought>

Nov 30 – A team of researchers from the University of Texas at Austin has used field testing and 3-D micro-CT imaging of laboratory experiments to show that rock salt can become permeable. Their findings, published in the 27 November issue of *Science*, has implications for oil and gas operations, and, most notably, nuclear waste storage. The team includes

researchers from the university's Cockrell School of Engineering and Jackson School of Geosciences.

“What this new information tells us is that the potential for permeability is there and should be a consideration when deciding where and how to store nuclear waste,” said Maša Prodanovi, assistant professor



CBRNE-TERRORISM NEWSLETTER – December 2015

in the Department of Petroleum and Geosystems Engineering. “If it’s an existing nuclear waste storage site, you may want to re-evaluate it with this new information.”

UTexas notes that salt generally blocks fluid flow at shallow depth, a feature that allows oil reservoirs to form. But scientists have long suspected that salt becomes permeable at greater depth. Jackson School professor James E. Gardner confirmed this theory through laboratory experiments with synthetic rock salt.

Cockrell School doctoral student Soheil Ghanbarzadeh tested the idea against field data from natural rock salt. During summer internships he examined

oil and brine distributions in rock salt in a set of forty-eight hydrocarbon wells owned and operated by Statoil. The observed fluid distributions confirm that salt indeed becomes permeable at greater depth. However, the researchers were surprised to find that fluids were sometimes able to flow through the salt at shallow depth.

In the study, they explain that deformation of rock salt may be the culprit. Deformation can stretch the tiny isolated pockets of brine that form between salt crystals and link them into a connected pore network that allows fluid to move.

Although this work was originally motivated by the desire to evaluate rock salt as a hydrocarbon reservoir seal for the oil industry, the conclusions may have important

implications for nuclear waste storage. Previous work on salt permeability has focused on the cracks induced by the creation of the nuclear waste repository itself. The observations reported by the study, however, demonstrate that undisturbed rock salt can become permeable.

“The critical takeaway is that salt can develop permeability, even in absence of mining activity,” said assistant professor Marc A. Hesse of the Jackson School’s Department of Geological Sciences. “Further work is necessary to study the quantity of flow that can occur.”

The Waste Isolation Pilot Plant (WIPP) in Carlsbad, New Mexico, stores low-level nuclear waste in salt

beds beneath the ground. However, high-level waste from the nation’s nuclear energy sector is stored at the power plants in pools or dry casks, methods that are considered temporary solutions. For decades there has been a proposal to build a permanent central repository under Nevada’s Yucca Mountains, but that proposal has stalled because of political and regulatory hurdles. This has renewed interest in rock salt as an alternative permanent storage solution for high-level nuclear waste. In this context, the findings of the team from UT Austin provide a timely reminder that rock salt is a dynamic material over long timescales.

Ghanbarzadeh hopes that “our discovery encourages others to ask questions about the safety of current and future disposal sites.”



— *Read more in Soheil Ghanbarzadeh et al., “Deformation-assisted fluid percolation in rock salt,” [Science](#) 350, no. 6264 (27 November 2015): 1069-72.*

Pegfilgrastim Approved for Treatment of Acute Radiation Syndrome

Source:http://www.domesticpreparedness.com/Government/Government_Updates/Pegfilgrastim_Approved_for_Treatment_of_Acute_Radiation_Syndrome/

Dec 05 - In November 2015, the Food and Drug Administration approved the use of pegfilgrastim (trade name Neulasta) to increase survival of people acutely exposed to high-dose radiation that damages the bone marrow. NIAID-funded research contributed to the approval of pegfilgrastim for treatment of acute radiation syndrome, which will improve access to the drug in the event of a public health emergency such as a nuclear power plant accident or terrorist attack.



CBRNE-TERRORISM NEWSLETTER – December 2015

Acute radiation syndrome occurs in stages following irradiation of the entire body by a high dose of penetrating radiation over a short period of time. Radiation exposure can injure multiple organs, and the rapidly dividing cells of the bone marrow are among the most sensitive to its effects. Radiation-induced bone marrow damage reduces the number of pathogen-fighting neutrophils and clot-forming platelets in the blood, which can lead to death from infection or excessive bleeding.

Scientists theorized that drugs used to replenish blood cells in certain cancer patients also may be effective treatments for acute radiation syndrome. Pegfilgrastim first received FDA approval in 2002 to reduce the chance of infection due to low white blood cell counts in cancer patients receiving certain types of chemotherapy.

Pegfilgrastim is the second radiation medical countermeasure to be approved under FDA's Animal Rule, a regulation that permits approval of some products based on efficacy testing in animals and safety testing in humans. FDA approved a similar drug, filgrastim (trade name Neupogen), for treatment of acute radiation syndrome in March 2015. While filgrastim is administered daily, pegfilgrastim is administered once a week, offering improved dosing convenience in a radiation public health emergency incident.

1 - 0.6 mL Single Use Prefilled Syringe

NDC 55513-190-01

AMGEN[®]**Neulasta**[®]
(pegfilgrastim)

Pegylated Recombinant Methionyl Human Granulocyte Colony-Stimulating Factor (PEG-r-metHuG-CSF) derived from *E Coli*

6 mg in 0.6 mL Single Use Prefilled Syringe**For Subcutaneous Use Only****Sterile Solution - No Preservative**

Manufactured by Amgen Manufacturing, Limited, a subsidiary of Amgen Inc.
Thousand Oaks, CA 91320-1799 U.S.A.

Rx Only

U.S. License No. 1080

6
mg

Both approvals were based on findings from NIAID-funded animal research indicating that these drugs are reasonably likely to increase survival of people with radiation-induced bone marrow damage. Because human efficacy testing could not be performed ethically, researchers developed and characterized a macaque model of acute radiation exposure. Administering pegfilgrastim nearly doubled survival: 91 percent of animals given pegfilgrastim survived 60 days after radiation exposure, compared to 48 percent without the drug. The pegfilgrastim group also experienced fewer gram-negative bacterial infections.

Approval of pegfilgrastim for treatment of acute radiation syndrome adds to the armamentarium of medical countermeasures available in the United States to address a possible radiological or nuclear emergency.

Questions Remain in “Final” Report on Iran’s Alleged Weapons Work

Source: <http://www.iranwatch.org/our-publications/nuclear-iran-weekly/questions-remain-final-report-irans-alleged-weapons-work>

Dec 10 – The International Atomic Energy Agency (IAEA) released its long-awaited final report on Iran’s alleged past nuclear weapons work on December 2. This report is likely to be the Agency’s last word on its investigation into what it calls “the possible military dimensions [PMD] to Iran’s nuclear program.” The Agency found that Iran had a “coordinated” program to develop a nuclear weapon through the end of 2003 and that some of the work on nuclear weapons continued into 2009.



CBRNE-TERRORISM NEWSLETTER – December 2015

Specifically, the IAEA found that Iran developed several components of a nuclear weapon and undertook related research and testing.



This report is part of a side agreement between the IAEA and Iran. The IAEA's conclusions are not directly linked to the implementation of the larger nuclear deal with Iran, which may explain the limited nature of Iran's cooperation. To many of the Agency's questions, Iran offered no new information, or made denials without explanation, or gave explanations contradicted by other information available to the Agency. The report sheds little new light on the allegations originally compiled by the Agency in 2011 and leaves unanswered many questions about the extent of both Iran's nuclear capability and its intentions.

Nevertheless, the countries of the P5+1 appear willing to accept the IAEA's incomplete report and close the book on the PMD issue. According to U.S. State Department spokesperson Mark Toner, the P5+1 will introduce a resolution at the next IAEA Board of Governors meeting on December 15 to bring the PMD investigation to an end. Iran, for its part, has stated that it will not implement the nuclear agreement, known as the Joint Comprehensive Plan of Action (JCPOA), until the IAEA investigation is concluded. In a November 29 interview, Iran's former defense minister and current secretary of the Supreme National Security Council warned that "without the closure of the file regarding past issues, there is no possibility of implementing the JCPOA."

The allegations about a nuclear weapons program in Iran began surfacing in 2002, and the IAEA consolidated the "outstanding issues related to possible military dimensions to Iran's nuclear program" in a report issued in November 2011. The analysis in the report was based on information that the Agency received from IAEA member states, from the Agency's own investigative efforts, and from information provided by Iran. The IAEA judged the allegations of work on nuclear weapons "to be, overall, credible" and "consistent in terms of technical content, individuals and organizations involved, and time frames." In a 2012 resolution, the IAEA Board of Governors

decided that "the resolution of all outstanding issues was essential and urgent in order to restore international confidence in the exclusively peaceful nature of Iran's nuclear program."

The 2011 IAEA report described detailed information about Iran's efforts to develop a nuclear weapon, including:

- computer modeling of implosion, compression, and nuclear yield, as recently as 2009;
- high explosive tests simulating a nuclear explosion but using non-nuclear material in order to see whether an implosion device would work;
- the construction of at least one containment vessel at a military site, in which to conduct such high explosive tests;
- studies on detonation of high explosive charges, in order to ensure uniform compression in an implosion device, including at least one large scale experiment in 2003, and experimental research after 2003;
- support from a foreign expert, reportedly a former Soviet weapon scientist named Vyacheslav Danilenko, in developing a detonation system suitable for nuclear weapons and a diagnostic system needed to monitor the detonation experiments;
- manufacture of a neutron initiator, which is placed in the core of an implosion device and, when compressed, generates neutrons to start a nuclear chain reaction, along with validation studies on the initiator design from 2006 onward;
- the development of exploding bridgewire detonators (EBWs) used in simultaneous detonation, which are needed to initiate an implosive shock wave in fission bombs;
- the development of high voltage firing equipment that would enable detonation in the air, above a target, in a fashion only making sense for a nuclear payload;
- testing of high voltage firing equipment to ensure that it could fire EBWs over the long distance needed for nuclear weapon testing, when a device might be located down a deep shaft;
- a program to integrate a new spherical payload onto Iran's Shahab-3 missile, enabling the



CBRNE-TERRORISM NEWSLETTER – December 2015

missile to accommodate the detonation package described above. The chart below details each of the 12 “outstanding issues” identified by the IAEA, and it explains their significance for nuclear weapons. It also lists the original evidence or basis for concern described by the IAEA in 2011, as well as any explanation offered by

Iran since then. It ends with the IAEA’s conclusion. For most of the 12 issues, the IAEA, in the absence of new information or meaningful disclosures from Iran, has merely reiterated the evidence contained in its 2011 report. This “final” report fails to present a complete picture of Iran’s past work on nuclear weapons.

- ▶ Read the full report [here](#).
- ▶ Read the accompanying chart [here](#).



The story of the man who saved the world

Source: <http://www.telegraph.co.uk/film/the-man-who-saved-the-world/nuclear-war-true-story/>



Col (ret'd) Stanislav Petrov



Man Gets 8 Years in X-Ray Weapon Plot That Targeted Muslims

Source: <http://abcnews.go.com/US/wireStory/man-years-ray-weapon-plot-targeted-muslims-35798889>

Dec 16 – An upstate New York man who admitted building a remote control for a mobile X-ray device intended to kill Muslims has been sentenced to eight years in prison.

Eric Feight, 57, of Hudson, pleaded guilty in 2014 to providing material support to terrorists. He was sentenced Wednesday in federal court in Albany.



Feight, a control systems engineer, told U.S. District Judge Gary Sharpe that co-defendant Glendon Scott Crawford first approached him to help create a mobile X-ray to sterilize medical waste, only later telling him it could be used to target Muslim terrorist cells operating in the U.S.

"Potential targets were never discussed with me," Feight said. The married father of three said he became afraid to drop out after Crawford introduced him to two seemingly dangerous investors in the project, actually FBI undercover agents.

He procrastinated for six months in delivering the remote control while refusing to integrate it to directly operate the actual X-ray machine the agents brought, adding he didn't think it would work, he said.

"You understood what it was you were doing," Sharpe said. The machine could have worked and killed people as intended, he said.

"It's bizarre somebody with your background, your intelligence and your experience would be listening to Crawford's nonsense," Sharpe said.

Feight's sentence was shorter than the 15 years prosecutors requested.

Crawford, 51, an industrial mechanic at General Electric in Schenectady, where Feight was a subcontractor, was convicted of attempting to produce a deadly radiological device, conspiring to use a weapon of mass destruction and distributing information about weapons of mass destruction. He could face 25 years in prison at his sentencing in March.

Investigators taped Crawford, a Navy veteran and also a family man with no criminal history, calling Islam "an opportunist infection of DNA" and approaching a Ku Klux Klan grand wizard who was an FBI informant for support with the X-ray.

Feight and Crawford were arrested in 2013 and have been jailed since.

Investigators began tracking Crawford in 2012 after he approached two Albany-area Jewish groups. Authorities said the device was inoperable. Nobody was hurt.



Booby-trapped dolls seized in Baghdad; Isis planned bomb blasts during Arbaeen

Source: <http://www.ibtimes.co.in/booby-trapped-dolls-seized-baghdad-isis-planned-bomb-blasts-during-arbaeen-655770>

Nov 20 – The Iraqi police have foiled a major bombing plot in Baghdad, where 18 dolls stuffed with bombs were seized by the security forces, which were meant to be scattered on the roads leading to Karbala during Arbaeen - a Shia Muslim religious observance.



Haidar Sumeri
@IraqiSecurity



Despicable. #Iraq's army find a number of children's dolls filled with explosives & ready to blow north of #Baghdad.

12:24 AM - 20 Nov 2015

498 134

Arbaeen, which this year will be held on December 3, is a Shia religious observance that occurs forty days after the Day of Ashura to commemorate the martyrdom of Husayn ibn Ali, the grandson of Prophet Muhammad.

During Arbaeen at least 20 million people walk to the city of Karbala in Iraq, making it one of the largest pilgrimage gatherings on Earth.

The booby-trapped bombs were discovered by the security forces in al-Husseiniya - a predominantly Shiite suburb in northeastern



Baghdad, Kuwait News agency (KUNA) reported.

According to Press TV, Isis was planning to plant the bomb on a roads towards Karbala from Baghdad.



CBRNE-TERRORISM NEWSLETTER – December 2015

The explosive-laden dolls were later dismantled and destroyed. At least 26 people were killed and dozens were injured on 13 November, after two Isis bombings in Baghdad.



Twenty-one people were killed after an Isis suicide bomber struck a funeral procession for a Shiite militia fighter killed in the Baghdad suburb of Hay al-Amal. The same day a roadside bomb planted near a Shiite shrine in Sadr City, killed at least five people and injured 15, New York Times had reported.

Bomb blast at Hellenic Federation of Enterprises offices in Athens

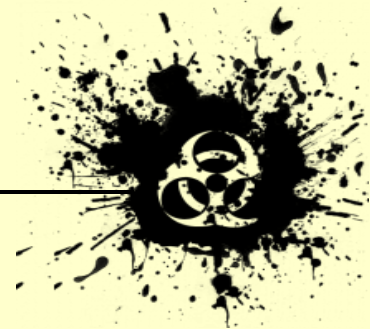
Source: <http://en.protothema.gr/bomb-blast-at-hellenic-federation-of-engerprises-offices-in-athens-pics/>



Nov 24 – An explosion at the offices of the Hellenic Federation of Enterprises (SEV) at 5 Xenofontos Street, Syntagma, shook the city center at 3.35 a.m. when the blast took place. A warning call had been made to Greek newspapers Vima and Efimerida ton Syntakton at 2.51 a.m. when an unknown man said that there would be a blast in 40 minutes.

Police and the fire brigade evacuated the area so there were no injuries. The blast was quite strong and there were calls from various areas around Athens concerning the explosion. The damage to the building and surrounding buildings are extensive.

Investigations are ongoing – involvement of “Nuclei of Fire” terrorist organization is suspected.



CBRNE-TERRORISM NEWSLETTER – December 2015

There has still been no organization claiming responsibility for the blast near a gas station and central hotel. The offices of the Hellenic Federation of Enterprises had been targeted in 2010 by the organization “Mideniki Anohi” (Zero Tolerance) and there have been 19 attacks in 4.5 years.

Russia Develops Landmine with ‘Electronic Brain’

Source: <http://i-hls.com/?p=66913>



Nov 24 – **Russia has developed new anti-personnel landmines with smart electronic brains that are capable of distinguishing between soldiers and civilians. The landmine goes off only when someone armed approaches it.** The all new **Medalyon POM-3** rules out any unauthorized diffusing or premature explosion, reported Sputnik News. **When activated, the landmine fires an explosive charge in a 360-degree horizontal arc.**

The landmine’s Russian-designed nanochip is almost impossible to crack. “Even if the enemy is lucky enough to get hold of the POM-3 and is still alive afterwards, he will never be able to figure out how it works,” The Scientific Research Institute of Engineering’s director Igor Smirnov told Russian TV. The head of the Institute’s department of munitions, mining and demining, Mikhail Zhukov, said that because of the mine’s electronic brain, the time of its self-destruction can be remotely set, changed or cancelled altogether.

The smart landmines have already cleared field tests, and will soon enter service with the Russian armed forces. Moscow isn’t just developing advanced military technologies. It is actively using them against the Islamic State in Syria. According to ValueWalk, Russia’s little-known self-aiming bomb called the SBPE has been found in Syria. The self-guided SBPE uses infrared guidance to track and strike tanks and other military equipment with “great precision.” The SBPE smart munitions are highly effective in destroying multiple targets like military equipment, as proven by several Russian attacks where troops destroyed 50 ISIS vehicles, and in another case they blew up 20 ISIS tanks.

CounterBomber®

Source: <http://www.rapiscansystems.com/products/counterbomber>

The CounterBomber® system combines radar and video technology to automatically detect concealed person-borne threats such as suicide vests and weapons, in real-time, at stand off distances. Deployed by security forces around the globe, the CounterBomber® system is capable of automatically detecting suicide vests and other person-borne threats at distances outside of the blast danger zone.





The result: threats are rapidly detected and mitigated before they can harm personnel or critical infrastructure.

CounterBomber® has been extensively tested by the US Government, and has been fielded to US Armed Forces as well as various International Security Forces at numerous locations world-wide. The CounterBomber® system is a proven security asset that provides un-matched protection at high-value locations such as federal buildings, mass transit hubs, hospitals, military bases, and energy plants.

SYSTEM FEATURES

The CounterBomber® system is easily and quickly assembled, and once in operation can be configured to assess personnel for threats automatically – with no operator interpretation. In addition, CounterBomber's intuitive and rugged design reduces training and maintenance costs,

and its plug-and-play functionality enables it to be quickly and securely integrated into the command and control (C2) network of virtually any security solution architecture.

SAVE LIVES THROUGH STANDOFF IED DETECTION

FEATURE	BENEFIT
Stand-Off Detection	Reduces risk to security personnel and saves lives
Highly Accurate (High Pd, Low Pfa)	Finds threats without bogging down screening operations
Intuitive and Easy to Use	Requires little operator training
Automatic Threat Detection	Reduces operator fatigue and frees up security personnel
Safe, Non-Imaging Assessment	Mitigates liability and privacy concerns
Easy to Integrate	Enables enhanced situational awareness and C2

CounterBomber® provides a powerful force protection capability by automatically and accurately detecting concealed threats at stand-off distances.

CounterBomber® is a video-steered radar sensor that utilizes cutting edge radar signal processing and video tracking technology to rapidly and accurately assess approaching personnel for the presence of concealed person-borne threats. While the system has been extensively tested by the United States Government for detection of suicide vests, CounterBomber® has also demonstrated the ability to detect other concealed threats such as handguns, machine pistols, etc. CounterBomber® has been successfully deployed operationally across the globe since 2007, and has been used in urban, suburban, and rural environments with equal success.

CounterBomber® can also readily integrate decision information and live-video streams into standard Command and Control systems for increased situational awareness among security personnel.

Detecting suicide bombers from a safe distance

Source: <http://www.homelandsecuritynewswire.com/dr20120504-detecting-suicide-bombers-from-a-safe-distance>

2012 – Suicide bombings have now spread to Syria; a Florida company produces equipment designed to aid in the detection of a suicide bomber at standoff distances, before a terrorist can reach his intended target



CBRNE-TERRORISM NEWSLETTER – December 2015

In a recent incident of a suspected suicide bomb plot, Israeli Defense Forces (IDF) captured a Palestinian with two explosive devices near a West Bank roadblock. The bombs were detonated at a controlled destination, and the terror suspect is being held for questioning.



That incident comes following a deadly suicide bombing in Syria that claimed at least nine lives in Damascus. An Islamic group identifying itself as al-Nusra Front claimed responsibility, saying its operative detonated his explosive in the midst of 150 Syrian security forces.

“We are fortunate the IDF was able to apprehend the suspected West Bank terrorist before tragedy could occur,” said Richard Salem, CEO of Tampa, Florida-based threat detection maker Thermal Matrix International. “But as we have seen in Syria, not all potential threats are being discovered in time.”

Thermal Matrix produces equipment designed to aid in the detection of a suicide bomber at standoff distances, before a terrorist can reach his intended target. The company says the technology can detect plastic, liquid, powder, and gel explosives, which may not be seen when hidden beneath clothing, nor detected by metal detectors at entry check points.

The company’s [ACT Threat Detection System](#) integrates with infrared sensors, aiding in concealed object threat detection through target identification, target tracking, and color analysis of potential



PBIEDs (person-borne improvised explosive devices). The company notes that the system also displays and controls the imagery of multiple sensors, adding the ability to record, review, and archive scenes at a safe distance.

The two most recent suicide bomb incidents are not isolated. In the West Bank alone, two Palestinians with four pipe bombs were arrested one week ago. Earlier in April another terrorist was detained, found to be in possession of seven improvised explosive devices. Officials were quoted as saying they suspected the Palestinian planned to attack Israeli civilians or soldiers during Passover.

“The threat situations we have seen over the past couple days are exactly the types of situations our technology can help defuse,” Salem said. “We expect these attempts to continue until we can demonstrate to terrorists that we have advance warning technology capable of stopping them.”




CBRNE-TERRORISM NEWSLETTER – December 2015

The company also notes that although the system aids in detecting what is hidden beneath clothing, it is not an x-ray. This means there are no invasion of privacy concerns since the technology does not depict any anatomical features.

Move over x-ray: Millimeter is wave of the future for Homeland Security

Source: <http://www.rec-usa.com/press/MM%20Wave%20Radar%20Move%20Over%20XRay.pdf>



RENAISSANCE
hxi Millimeter Wave Products
The New Thinking in Wireless Technology

**Move Over X-ray:
Millimeter is Wave of the Future for Homeland Security**

Millimeter wave stand-off detection systems currently being developed under a contract from the Department of Homeland Security are designed to detect suicide bombers at a distance

There is a growing and critical need for the detection of person-borne improvised explosive devices (PBIEDS). A favored tactic due to its simplicity and low cost, suicide bombing creates maximum fear because the victims are randomly chosen, and in public areas such as schools, churches, hospitals, sports stadiums, bus or train stations, or other populated areas.

Standoff IED, Person-Borne & Vehicle-Borne Explosives & Weapon Detection: Technologies & Global Market - 2015-2020

Source: <http://www.prnewswire.com/news-releases/standoff-ied-person-borne--vehicle-borne-explosives--weapon-detection-technologies--global-market--2015-2020-300103631.html>

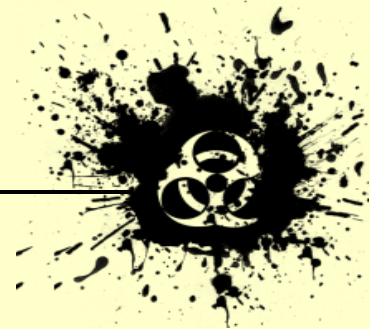
June 23 – Terrorist attacks using IEDs, Person-Borne IEDs (PBIED) and Vehicle-Borne IEDs (VBIED) have peaked in 2007 due to the U.S. & NATO wars in Afghanistan and Iraq. While the withdrawal of the U.S. from these countries resulted in a decline of VBIED & PBIED attacks, we now face a new surge of suicide attacks which are growing at an alarming rate

In 2014 alone, there were 424 confirmed PBIED & VBIED suicide attacks – an increase of 90% over the 223 suicide attacks in 2011 – causing the death of 3,554 people by 2014 vs. 2,027 in 2011.

IED, PBIED and VBIED attack threats are now a global problem, driving a growing number of security and defense forces to acquire cutting-edge standoff IED, PBIED & VBIED detection equipment. The purpose of standoff PBIED, VBIED and weapon detection technologies is to determine at a safe distance if a human subject or a vehicle is carrying explosives or weapons. Concealed explosives detection is perceived as one of the greatest challenges facing the counter-terror and military communities. The threat posed by suicide bombers is the key to the emergence of transformational counter-terror technologies and tactics. The maturity and deployment of advanced standoff detection technologies, capable of detecting suicide and other terrorists at a safe distance, will change the landscape of homeland security and asymmetric warfare.

In the new "Standoff IED, Person-Borne & Vehicle-Borne Explosives & Weapon Detection: Technologies & Global Market – 2015-2020? Report we forecast that the **cumulative 2015-2020 revenues will reach \$8.4 billion.**

The report, segmented into 120 sub-markets, offers for each sub-market 2013-2014 data and 2015-2020 forecasts and analyses. In 340 pages, 113 tables and 200 figures, the report analyzes and projects the 2015-2020 market.



CBRNE-TERRORISM NEWSLETTER – December 2015

According to the report, the market growth is boosted by the following drivers: Strengthening of radical Islamist IED, PBIED & VBIED attacks and threats in the Middle East, Africa, Europe and the U.S. The 2011-2014 growth of PBIED & VBIED suicide attacks Investments of defense forces around the globe in asymmetric warfare equipment Introduction of advanced standoff IED, PBIED & VBIED detection devices, technologies and systems Ever-growing profit of after-sale business (e.g., maintenance, upgrades and refurbishment).

The report examines each dollar spent in the market via 3 orthogonal money trails: 5 regional, 6 technological and 4 by revenue source markets.

This "Standoff IED, Person-Borne & Vehicle-Borne Explosives & Weapon Detection: Technologies & Global Market – 2015-2020" report is a valuable resource for executives with interests in the market. It has been explicitly customized for industry, security and military decision-makers allowing them to identify business opportunities, developing technologies, market trends and risks; as well as to understand the industry solutions to the threats of suicide terror, and to benchmark business plans.

Questions answered in this 340-page mega report include:

What will the market size be in 2015-2020?

What are the main standoff IED and weapon detection technology trends?

Where and what are the market opportunities?

What are the market drivers and inhibitors?

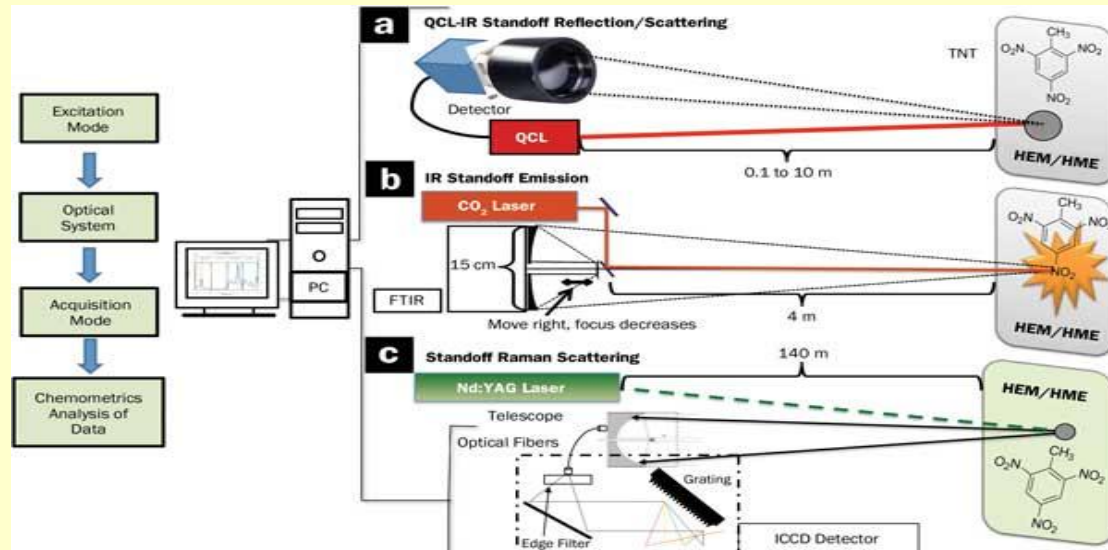
Who are the key vendors, their products and policy?

What are the challenges facing the standoff IED and weapon detection market entrants?

Handheld infrared camera use for suicide bomb detection: feasibility of use for thermal model comparison

By Dickson, Matthew R; MSc.Thesis – 2008)

Source: <http://krex.k-state.edu/dspace/handle/2097/1045>



One of the most deadly tactics used by today's terrorists is suicide bombing. Sensors have been developed and are being used in different situations to detect weapons and the people initiating suicide bombing attacks. The ideal detection technology would be fast, accurate, effective from long distances, and safe for the both detector and the object being detected. One detector that has shown potential as a tool for detecting hidden weapons is an infrared detector. **Infrared detectors** are passive sensors that create infrared, or thermal, images without having to expose the subject to any radiation. These images show the heat signature that is given off by objects of interest. Previous studies using infrared detectors for concealed weapon detection have tried to observe the image of the weapon. These have been largely unsuccessful, however, because infrared waves will not readily penetrate clothing.



CBRNE-TERRORISM NEWSLETTER – December 2015

The research presented here determines the feasibility of modeling the heat signature produced by a suicide bomber using thermal models that predict the temperature of the exterior layers of clothing worn. The goal is to be able to compare the images acquired of the suspected bomber to the expected temperatures from the thermal models. If the presence of a hidden weapon affects the emitted heat signature to a point in which the clothing temperatures are not responding as predicted by a model, it is possible a detection system may be created using these models as a comparator and signal for detection.

This research also determines a temperature range for which an operator viewing infrared images for suicide bomb detection may be relatively certain of the presence of a foreign object. Testing was also completed to determine those variables that affect an infrared image in ways that help or hinder the use of the thermal models in predicting the temperatures that appear in the infrared images.

A compressed sensing approach for detection of explosive threats at standoff distances using a Passive Array of Scatters

Homeland Security Affairs; Supplement 6, Article 1 (April 2013 – www.hsaj.org)

Source: <http://wp.vcu.edu/hsep/files/2013/06/A-compressed-sensing-approach-for-detection-of-explosive-threats-at-standoff-distances-using-a-Passive-Array-of-Scatters.pdf>

A compressed sensing approach for detection of explosive threats at standoff distances using a Passive Array of Scatters

Jose Angel Martinez-Lorenzo, Yolanda Rodriguez-Vaqueiro and Carey M. Rappaport
ALERT Center of Excellence for Department of Homeland Security,
Gordon CenSSIS, Northeastern University Boston (MA), USA
{ jmartine ; rappapor }@ece.neu.edu

Oscar Rubinos Lopez, Antonio Garcia Pino
Dept. of Signal Theory and Communications, University of Vigo, Vigo, Spain
{ oscar ; agpino }@com.uvigo.es

The sensor that can sniff out a suicide bomber from 100 metres away: Scanner could be built into public places

Source: <http://www.dailymail.co.uk/sciencetech/article-3327343/The-tool-sniff-suicide-bomber-100-metres-away-Multi-sensor-device-shows-abnormalities-holes-images.html>

Nov 20 – **The U.S. military is working on improving a device that could be used to detect concealed bombs and suicide vests such as those used in last week's tragic Paris attacks from more than a football field away.**

An earlier version of the multi-sensor technology, which is called the Standoff Suicide Bomber Detection System, or SSBDS, was used in Afghanistan in 2012 according to Defense One.

The device is 'limited by physics,' so it can't be designed as a handheld tool, but has the potential to be incorporated into the architecture of high-traffic public buildings, like train stations or stadiums.

HOW IT WORKS

The Standoff Suicide Bomber Detection System (SSBDS) measures midwave and longwave radiation, as well as the terahertz wavelength, through multiple sensors.

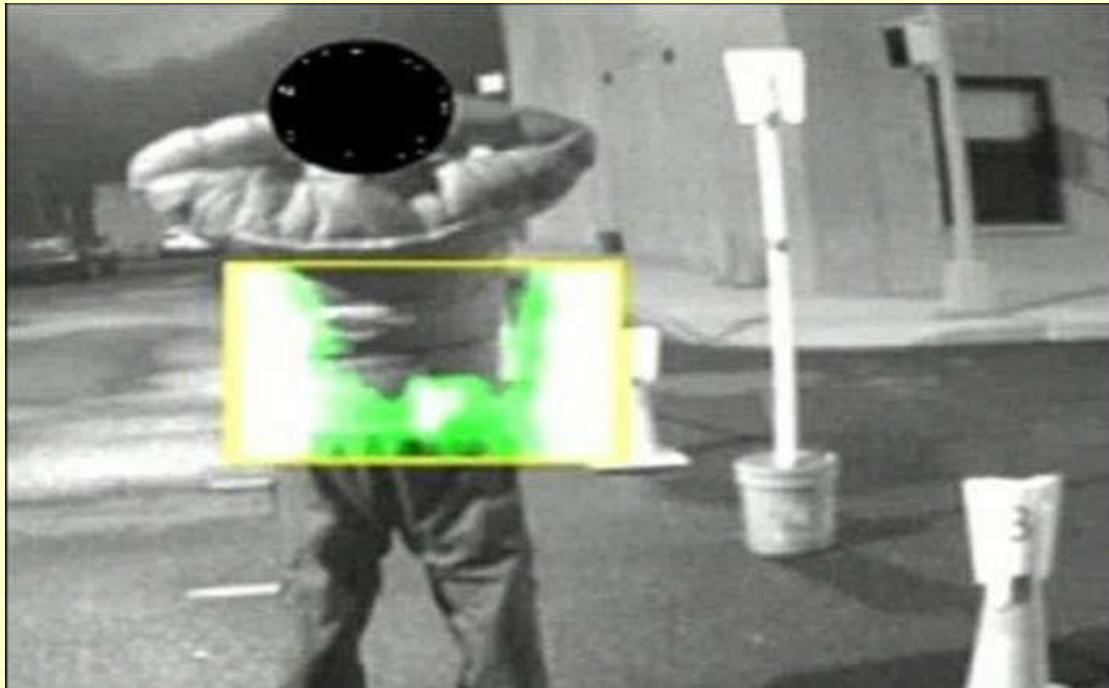
The device shows images through different views: black and white infrared, bright orange terahertz, and standard.

Abnormalities, like a concealed bomb in a suicide vest, show up on the sensor as dark spots of negative space, or holes where there should have been orange or white.



CBRNE-TERRORISM NEWSLETTER – December 2015

To improve the device, developers are looking to incorporate hyperspectral imaging, which will cut down on false positives and increase the detection range.



The SSBDS incorporates a multitude of sensors, which measure midwave and longwave infrared radiation, and the terahertz wavelength.



It is low energy and isn't ionizing, making it less dangerous than an X-ray, and also contains a visible-light camera.

If a person is hiding an explosive underneath clothing, the abnormality will appear as a dark area of negative space where there should be white or orange. 'It's a perfect system for dual use with Department of Homeland Security. Just think of Paris,' a JIDA scientist told Defense One

Researchers of the Joint Improvised-Threat Defeat Agency, or JIDA, first

developed the system to protect troops on forward operating bases.

Increasing instances of terrorist attacks in civilian areas now necessitates these kinds of devices outside of a military setting.

'It's a perfect system for dual use with Department of Homeland Security. Just think of Paris,' a JIDA scientist told Defense One.

The SSBDS stands at around three feet tall and offers three views when directed toward a person: a black and white infrared view, bright orange terahertz view, and a regular picture.

If a person is hiding an explosive underneath clothing, the abnormality will appear as a hole, a dark area of negative space where there should be white or orange.

'We can take different materials, such as your jacket, my jacket, her shirt. Although they're very similar in material makeup they actually have their own unique signature, just like a fingerprint,' says another scientist.

The system is operated by trained personnel to locate the dark spots on the sensor, but trials in Afghanistan revealed that sunlight can interfere with the terahertz sensor.



CBRNE-TERRORISM NEWSLETTER – December 2015

Researchers are now working on making it more precise by integrating a new, cutting-edge sensor for hyperspectral imaging. Developers are waiting on research-and-development money before this can be incorporated.

Hyperspectral imaging would increase the range and limit the number of false positives detected by the device, and, it would allow operators to potentially identify the presence of explosives, not just dark spots.

At its current stage in development, an SSBDS is expensive; a system could be more than a million dollars, but the price could drop as the device becomes more commercial.

The Tianjin Explosion

By Tuan Vu (Chemical Emergency Responder)

Source: <http://the-ncec.com/the-tianjin-explosion/>



Nov 16 – Nearly 2 months have passed since the Tianjin incident that had a significant impact not only locally, but on the supply chain of global companies. In this blog we assess and evaluate what impact it has had and what do companies need to do in order to learn from this tragic event.

What happened?

Around 11pm local time (3pm GMT), a fire was reported at the Ruihai Logistics site within the Binhai area of Tianjin Port. Firefighters attending the scene proceeded to control the fire using water sprays, however they were unaware of the dangerous goods on site. As a result, several chemical reactions took place causing an initial explosion in the area shortly before midnight local time (4pm GMT). Roughly **30 seconds later, a much larger secondary explosion had occurred with a blast equivalent to 21 tons of TNT. There were over 100 fatalities with more than 600 injured and many (mostly firefighters) remain missing.** The blast radius had caused significant damage to businesses and

properties up to 5km from the epicenter. The cause of the incident remains under investigation.

What went wrong?

The site stored around 3000 tons of over 40 different hazardous chemicals which consisted of, but not limited to, calcium carbide, potassium nitrate, ammonium nitrate and sodium cyanide. Well over the limit that its license had permitted. Firefighters who arrived on scene first were unaware of the dangerous goods on site and were using water to douse the fire. It is likely that Calcium carbide (used in the manufacture of acetylene gas and fertilisers) reacted violently with the water,



CBRNE-TERRORISM NEWSLETTER – December 2015

giving off flammable acetylene gas which intensified the fire and detonated the ammonium nitrate. 800 tons of ammonium nitrate were found, an oxidizing substance that can cause or contribute to the combustion of a substance. If involved in a fire, it decomposes explosively and detonates without warning which consequently produced the second explosion.

What impact did this have?

The incident had impacted people, property, business and the environment. This had led to claims totaling more than USD 1.5 billion for both national and international insurance companies and widespread global media coverage.

Death and personal injuries had an impact on productivity. At the time of this report, the death toll had risen to 135, more than 600 are injured and several remain missing. Families of the injured and dead will have been demoralized, as many protested against the company and the Chinese state government for the damages



caused to their families, homes and community.

Significant damage caused many homes, businesses and public buildings to be rendered inaccessible and unsafe for work. Road/rail infrastructure and marine property at the port were also damaged by the fire which had an effect on operations. At present, the area is still being cleared of debris and it will be several months until the area is rebuilt and redeveloped for use. From pictures, there is a vast quantity of expensive equipment, shipping containers and cargo that had been affected. Owners of the cargo passing through Tianjin will be looking to determine if their cargo had been affected.

Interruption to all business in the blast zone will leave companies and families with significant losses, especially multinational corporations who trade in the area daily with high value goods and services. It is expected that production at manufacturing sites would be delayed until they can confirm the safety of its facilities and the surrounding areas.

The Tianjin port is the third largest in China and fourth largest in the world for total cargo throughput, and this incident will have caused major disruption to many services and operations. Such that terminal areas at the port had to divert vessels, which increased the cost for operators and caused customer dissatisfaction.

A vast quantity of harmful pollutants had entered the atmosphere putting the public at risk of experiencing breathing difficulties. It was confirmed that hydrogen cyanide, hydrogen sulfide, carbon monoxide, nitrogen oxide and other volatile organic compounds were present within 500m from the epicenter, which are toxic if inhaled. Many, if not all persons were

required to wear face masks with firefighters wearing breathing apparatus' to help deal with the fire and debris.

Sodium cyanide was also detected in sewers and some waterways, with results exceeding the limit of cyanide concentration in water. It was reported that hundreds of dead fish had washed up on shore, which raised the question of whether there will be traces of cyanide in water and food. The chemical is toxic to aquatic organisms and can bioaccumulate in

the food chain. This will have impacted people in the longer term that will lead to health problems or worsen existing problems.

What impact did this have indirectly?

In addition to the immediate impacts of the explosion, there will have been many indirect impacts. The fact that companies and market analysts admit they did not know the extent of this impact, several weeks after the event, shows the complex nature of this large-scale accident. Aggravating factors may have included the host nation's reluctance to give companies early access or release of information; and the event occurred against a backdrop of



CBRNE-TERRORISM NEWSLETTER – December 2015

dramatic instability in Chinese markets. But we must accept that these major incidents will occur periodically, and that the ripples from such an event will impact companies in some way.

What can companies do about it?

If there is a phrase being used more than any other in boardrooms across the region right now it will probably be 'supply chain'. Perhaps the first thing companies can do is to understand their supply chains – all the dependencies, interdependencies, points of failure, redundancies – and to understand the quality of their supply chains. For example, investigating the nature of the organisations, linkages and relationships that make up supply chains. If companies genuinely do this, they will know how their supply chains work, both in business-as-usual mode and under stress.

It may be that the China regulatory environment is less mature than some other jurisdictions, but it is unlikely this will change fast. It is more likely that companies will need to understand and acknowledge the imperfect relationships they have in these cases, and work transparently to manage and improve them. It may be that threats to business appear to be growing - terrorism, cybercrime, extreme weather might suggest this trend – but actually major industrial incidents are no more likely to occur than before, and much has been done by industry to reduce their likelihood and consequence. What companies *can* influence is their resilience.

Whatever the eventual value placed on direct and indirect losses, the figures will be in millions and billions of dollars. Some companies will weather this storm better than others: they will have been more resilient and

achieved continuity of business. They may just have been lucky, but more likely they will have achieved this by understanding how their supply chain works ... and doesn't work. Having this knowledge allows companies to make good decisions about risk transfer, risk sharing, risk reduction; and allows them to make contingency plans and recovery strategies that will work in the next crisis.

NCEC's Emergency Responder had received a call from one of our private sector clients' on their crisis notification line. They informed that many of their empty product tanks awaiting return to the USA had been affected by the explosion. The tanks were labelled as hazardous and contained residues and therefore needed to be treated as hazardous materials. NCEC's responder relayed the information to one of the company's dedicated contacts for the region who dealt with the issue.

What could have been done differently?

Responders could have performed a more thorough risk assessment whilst in transit to the site. This would look at questioning civilians in the area or the initial caller to determine what materials were on-site, so they could identify the right firefighting material to use without putting more people at risk.

After assessing the risk associated, an initial evacuation of the immediate area would increase saveable life and assist those who are already injured.

Effective communication between multi-agency groups could have allowed better co-ordination of tasks and priorities in order to treat those injured, whilst being a considerable distance away from the site to reduce any risk to their own safety. More investment into emergency services for training would aid a more effective response in the wake of a disaster.

Fake bomb detectors used to protect Sharm Britons: Gadgets similar to novelty golf ball finders that were part of UK fraud trials are being used to check luggage at resort's hotels

Source: <http://www.dailymail.co.uk/news/article-3311097/Fake-bomb-detectors-used-protect-Sharm-Britons-Gadgets-similar-novelty-golf-ball-finders-UK-fraud-trials-used-check-luggage-resort-hotels.html>

Nov 09 – **British families in Sharm El Sheikh are being guarded with useless bomb detectors based on a bogus device produced by UK fraudsters, the Mail can reveal.**

Hotels are using the fake gadgets – now produced by the Egyptian army – to screen luggage amid fears of bomb attacks by Islamic State terrorists.



CBRNE-TERRORISM NEWSLETTER – December 2015

But they are almost identical to a completely useless device, based on a novelty golf ball detector, at the centre of fraud trials in Britain over the past two years. Experts say they are just radio aerials stuck to handles.



The revelation comes as Egyptian police investigate whether a Sharm hotel worker might be responsible for a suspected attack on a Russian passenger jet. Police fear a bomb may have been smuggled inside luggage.

Bogus: A guard, seen from a hidden camera, using the device at Sharm's Savoy Hotel

As thousands of UK families were still waiting to fly home yesterday, the Mail discovered fraudulent 'scanning devices' were being used to protect at least five top hotels packed with Britons. Security guards use them to 'sweep' guests, their cars and luggage.

But experts say these 'screening tools' are almost identical to the bogus devices produced by British fraudsters and sold for millions to foreign governments, resulting in prosecutions in 2013 and 2014.

The Egyptian army appears to have copied these devices and produced its own version called C-Fast, which is being used across Sharm.

It means a terrorist bomb could easily have been smuggled

into a hotel, put in a passenger's luggage and potentially taken on to a plane. Since C-Fast devices are made by the Egyptian army, it is likely they are also used at Sharm's airport.

Last night the Foreign Office and British holiday companies, were looking into the revelations – which come after a security expert who had recently visited Sharm contacted the Daily Mail to warn that fake bomb detectors were being used at the resort.

They said: 'They are utterly useless devices which have no better chance of detecting bombs than random chance.'

On Sunday, the Mail saw the devices used at three hotels. At the Savoy, where UK Ambassador John Casson has held meetings, alongside British tourists, one was being used to check vehicles. Similar devices were in operation at Sultan Gardens, used by EasyJet and Thomas Cook, and Hilton Dreams, used by EasyJet and Monarch. Yesterday, the 'detectors' were used at the Hilton Fayrouz and Xperience St George Homestay.



CBRNE-TERRORISM NEWSLETTER – December 2015

Research showed C-Fast devices were patented as 'screening tools'. In the application, four years ago,



an Egyptian army scientist claims the device 'can detect any material' from up to 500 metres away, using 'static energy from the human body'.

Last night, Cambridge University physicist Michael Sutherland, an expert witness in the trials involving golf ball finders sold as bomb detectors, said the C-Fast 'appears to be nearly identical' to the devices discredited in the UK.

He said the patent made 'outrageous claims ... not backed up by any creditable scientific research', adding:

'It is quite simply a fraud, and a dangerous one ... They would have as much luck searching for explosives using a kebab'.

DEADLY DEVICE IS BASED ON A £13 GOLF GIMMICK

The fake bomb detector scam was one of the most successful – and dangerous – in history. Brazen con artists used a £13 novelty 'Gopher' golf ball finder, which itself does not work, to create a device they sold for up to £10,000 a time to governments around the world.

The detectors had no working parts and no power source, and the supposed theory behind them was described in a series of Old Bailey fraud trials as an 'affront to science'.

Yet they were sold for sums totaling some £100million to military forces either utterly credulous or desperate to protect themselves against terrorism, or in on the scam and taking kickbacks from the conmen.

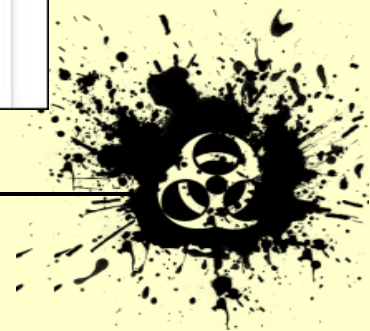
Hundreds of civilians may have been killed as a result of the devices' use in countries such as Iraq, where suicide bombers will have been able to pass security screening with ease.

The Britons involved in the scam, which began in the early 2000s, were James McCormick of Somerset, who made up to £50million; Gary Bolton, of Kent, said to have reaped £45million; Antony Williamson of Gosport; and pensioners Sam and Joan Tree, who put hundreds of the empty plastic devices together in a shed in Dunstable, Bedfordshire.

McCormick, 59, was jailed for ten years in 2013, and Bolton, also 59, for seven years. Williamson, 60, got two years suspended, and last year Mr Tree, 69, was jailed for three and a half years and his wife, 63, got a two-year suspended sentence.

C-Fast "HIV Detector"

FAKE Bomb detector ADE 651 sold to Iraq...



Global Landmine Casualties Increase, Afghanistan Largely to Blame: Study

Source: <http://m.ndtv.com/world-news/global-landmine-casualties-increase-afghanistan-largely-to-blame-study-1248701>



Cambodian Landmine Museum

Nov 29 – Long-term progress in reducing the number of landmine casualties was reversed last year, and rebel groups used the mines in 10 countries, the largest number since 2006, researchers said on Thursday. Non-state groups were still using the deadly devices in the 12 months to October 2015 in Colombia, Libya, Myanmar, Pakistan, Syria and Yemen, and in Afghanistan, where there was a sharp increase in casualties from improvised explosive devices (IEDs).

Landmines were also used by rebels in three countries - Iraq, Tunisia and Ukraine - where they were not used last year, and by three states: Myanmar, Syria and North Korea.

"While the world has made great progress, the past year has seen disturbing steps backward in terms of new use of and casualties from landmines," said Jeff Abramson, editor of the study, which was carried out by the International Campaign to Ban Landmines, a lobby group.

A total of 3,678 people were killed or wounded by landmines over the last year, about 10 per day. This is up from 3,308 in 2013 but far lower than in 1999, the year a major treaty came into force, when there were around 25 casualties each day.

The true figure is likely to be higher than the one recorded, but the drop is still highly significant because recording has improved over time, Thursday's report said.

The vast majority - about 80 per cent - of reported casualties were civilians.

"The new use of antipersonnel mines by non-state armed groups in ... Ukraine and Yemen, and the continuing large-scale use of victim-activated IEDs in Afghanistan and Iraq, are particularly worrisome," said Mark Hiznay, senior researcher at Human Rights Watch.

New landmines were laid in only a small minority of countries, but existing ones are still present in 57 nations. Mozambique declared



CBRNE-TERRORISM NEWSLETTER – December 2015

itself mine-free in September, the 28th country to do so since 1999.

At least 200 square kilometers of mined areas worldwide were reported cleared last year, most of them in Afghanistan, Cambodia and Croatia, a slight increase from 2013.

The 1999 Ottawa Convention prohibits the use, stockpiling, production and transfer of anti-personnel landmines. While backed by most countries, the treaty has not been endorsed by the United States, Russia, China and India.

Detecting, identifying explosives with single test

Source: <http://www.homelandsecuritynewswire.com/dr20151210-detecting-identifying-explosives-with-single-test>



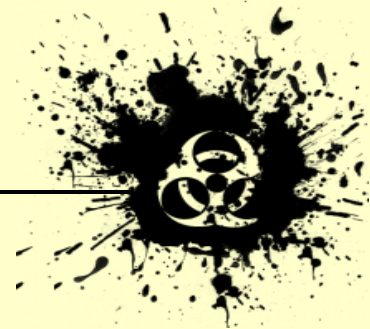
Dec 10 – A new test for detecting multiple explosives simultaneously has been developed by University College London (UCL) scientists. The proof-of-concept sensor is designed quickly to identify and quantify five commonly used explosives in solution to help track toxic contamination in waste water and improve the safety of public spaces.

Lead researcher, Dr. William Peveler (UCL Chemistry), said: “This is the first time multiple explosives have been detected using a single sensor before demonstrating proof-of-concept for this approach. Our sensor changes color within ten seconds to give information about how much and what explosives are present in a sample. Following further development, we hope it will be used to quickly analyze the

nature of threats and inform tailored responses.”

UCL reports that the study, published in *ACS Nano* and funded by the Engineering and Physical Sciences Research Council (EPSRC), used a **fluorescent sensor to detect and differentiate between DNT, TNT, tetryl, RDX, and PETN by reading unique color change “fingerprints” for each compound.**

Dr. Peveler, added: “We analyzed explosives which are commonly used for industrial and military purposes to create a useful tool for environmental and security monitoring. For example, DNT is a breakdown product from landmines, and RDX and PETN have been used in terror plots in recent years as they can be hard to detect using sniffer dogs. Our



CBRNE-TERRORISM NEWSLETTER – December 2015

test can quickly identify these compounds so we see it having a variety of applications from monitoring the waste water of munitions factories and military ranges to finding evidence of illicit activities.”

The sensor is made of quantum dots, which are tiny light-emitting particles or nanomaterials, to which explosive targeting receptors are attached. As each explosive binds to the quantum dot, it quenches the light being emitted to a different degree. The distinct changes in color are analyzed computationally in a variety of conditions to give a unique fingerprint for each compound, allowing multiple explosives to be detected with a single test.

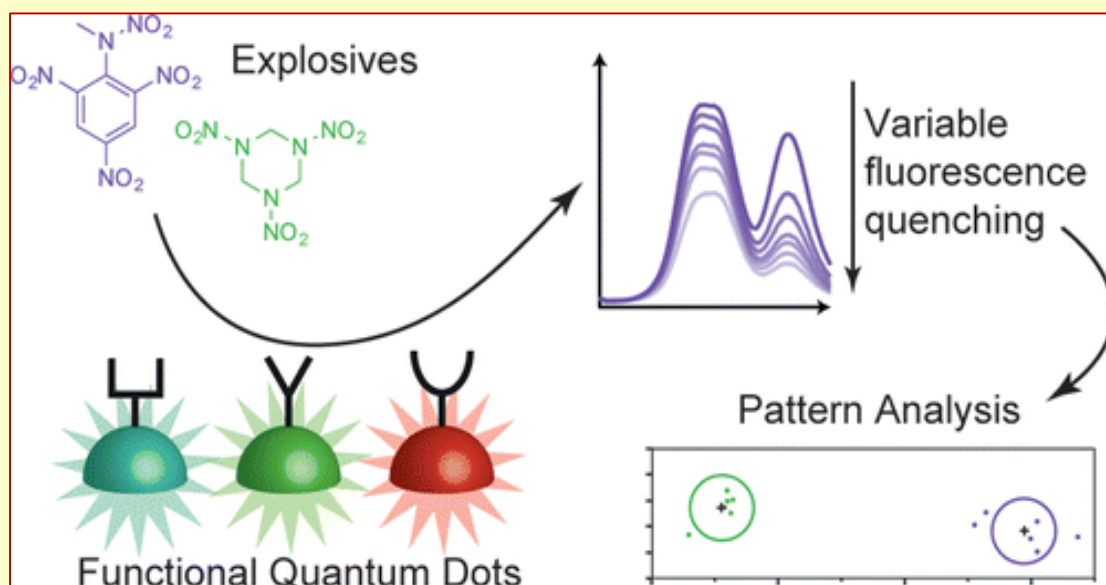
Senior author, Professor Ivan Parkin (UCL Chemistry), said: “Our sensor is a significant step forward for multiple explosives detection.

The sensing and differentiation of explosive molecules is key for both security and environmental monitoring. Single fluorophores are a widely used tool for explosives detection, but a fluorescent array is a more powerful tool for detecting and differentiating such molecules. By combining array elements into a single multichannel platform, faster results can be obtained from smaller amounts of sample. Here, five explosives are detected and differentiated using quantum dots as luminescent probes in a

Current methods can be laborious and require expensive equipment but our test is designed to be inexpensive, fast and use a much smaller volume of sample than previously possible. Although all of these factors are important, speed and accuracy are crucial when identifying explosive compounds.”

The team plan to take it from the laboratory into the field by blind testing it with contaminated waste water samples. They also hope to improve the sensitivity of the test by tailoring the surfaces of the quantum dots. Currently, its limit is less than one part per million which the team hope to increase into the part per billion range.

UCL notes that the funding from the EPSRC was provided through [UCL SECREt](#), a £17.5 million international doctoral center for Ph.D. training in security and crime science.



multichannel platform: 2,4-dinitrotoluene (DNT), 2,4,6-trinitrotoluene (TNT), tetryl (2,4,6-trinitrophenylmethyl nitramine), cyclotrimethylenetrinitramine (RDX), and pentaerythritol tetranitrate (PETN). The sharp, variable emissions of the quantum dots, from a single excitation wavelength, make them ideal for such a system. Each color quantum dot is functionalized with a different surface receptor via a facile ligation process. These receptors undergo nonspecific interactions with the explosives, inducing variable fluorescence quenching of the quantum dots. Pattern analysis of the fluorescence quenching data allows for explosive detection and identification with limits-of-detection in the ppb range.

— Read more in William Peveler et al., “Multichannel Detection and Differentiation of Explosives with a Quantum Dot Array,” [ACS Nano](#), Article ASAP (18 November 2015).



Matching bullets to wounds using organ-specific protein signatures found on projectiles

Source: <http://www.homelandsecuritynewswire.com/dr20151210-matching-bullets-to-wounds-using-organ-specific-protein-signatures-found-on-projectiles>

Dec 10 – **U Tübingen researchers have developed a method which enables them more accurately to reconstruct crimes involving sharp blades or firearms.** An interdisciplinary team from the Center for Bioinformatics Tübingen (ZBIT), Forensic Medicine, the Center for Quantitative Biology (QBIC), and bioanalysts from the Research Center for Ophthalmology (FIA) used traces of organic material found on bullets or other weapons used in crimes. Their findings are published in the latest edition of *Journal of Proteome Research*. Forensic medicine has long employed molecular biology to link, for instance, tiny amounts of organic material to a suspect. Yet, such methods are less useful when it comes to finding out which shot or stab wound was the cause of death. They enable a weapon to be linked to the victim, but not the projectile to the wound. This is sometimes necessary for the full reconstruction of a crime and presentation of evidence — for example, in cases where several people were involved in a shoot-out.

U Tübingen reports that the study's lead authors, Dr. Sascha Dammeier (FIA), Dr. Sven Nahnsen (QBIC), and Johannes Veit (ZBIT), used proteome analysis — which is based on mass spectrometry — to demonstrate that



projectiles which have been fired through vital organs bear traces of organ-specific proteins. These protein “signatures” allow experts to identify which organ the projectile passed through — and even match a bullet to the wound it caused.

The researchers initially tested the process on isolated cattle organs, which have typical protein patterns which can be statistically classified. Then the bullet metal was tested for relevant parameters.

After experiments showed that a majority of the protein signatures were clearly in evidence, the method was put to the test in a real murder case. Unfortunately, the purely bioinformatical classification yielded no clear result due to contaminants. Yet the identification of organ-specific proteins on several projectiles enabled forensic scientists to match all wounds to projectiles using a process of elimination. And this led to a complete reconstruction of the crime.

UT notes that the method has been patented and licensed. The Tübingen researchers hope that it will be widely used to compile a forensic database which will successively make the protein signatures of all important organs — and their combinations — available to forensic experts, so that the signatures can be quickly and effectively identified.

— *Read more in Sascha Dammeier et al., “Mass-Spectrometry-Based Proteomics Reveals Organ-Specific Expression Patterns To Be Used as Forensic Evidence,” [Journal of Proteome Research](#), Article ASAP (23 November 2015).*



Scots charity clears 200,000 landmines from Sri Lanka

Source: <http://www.bbc.com/news/uk-scotland-35072384>



Dec 11 – A Scottish charity has reached a significant milestone in its efforts to clear a former war torn part of Sri Lanka of landmines.

The **Halo Trust**, based at Thornhill in Dumfries and Galloway, announced that it has cleared 200,000 landmines in the country.

The project is thought to have helped 150,000 people return home after years



CBRNE-TERRORISM NEWSLETTER – December 2015

of displacement due to the country's civil war.

Damian O'Brien, the charity's programme manager in Sri Lanka, told BBC Scotland that there is much work to be done in order to meet the country's landmine-free deadline of 2020.

From Halo Trust website

<http://www.halotrust.org/where-we-work/sri-lanka/problem>

On 20 May 2009 the Sri Lankan Government declared an end to more than two decades of armed conflict with the Liberation Tigers of Tamil Eelam (LTTE), who had been seeking a separate homeland, or 'Eelam', for Tamils in the north and east of the country.

Landmines were used by both sides at different stages of the conflict and they continue to present an obstacle to the safe return of displaced families. Mines also block access to paddy fields, fishing jetties, grazing land and community infrastructure in villages throughout the North.

Most mines are of the anti-personnel type, sometimes laid in dense, patterned mine belts. There is also widespread nuisance mine-laying in residential areas, a common tactic of the LTTE, while unexploded and abandoned ordnance presents a threat across the North.

The number of mine casualties from 1985-2013 is reportedly around 22,000. The annual casualty rate rose in 2010 as the number of returnees increased and records suggest people are most at risk when planting crops or when harvesting. Other high risk activities include collection of scrap metal and firewood and whilst foraging, fishing or hunting. The numbers of accidents have declined gradually since 2010. Sri Lanka has not acceded to the Mine Ban Treaty.



Is cyber terrorism an imminent danger or merely Hollywood fiction?

Source: <http://www.smh.com.au/national/is-cyber-terrorism-an-imminent-danger-or-merely-hollywood-fiction-20151111-gkwh5s.html>

In August this year, as thousands of US punters prepared to wager their wallets on which horse would win a race called the \$1 Million TVP Pacific Classic, online betting agency Xpressbet crashed and burned.

In a statement issued the next day the business revealed it had been the victim of a type of digital sabotage known as a Distributed Denial of Service (DDoS) attack.

Essentially, the company's computer system had been flooded by millions of simultaneous incoming messages, upon receiving which – to use the technical term – it shat itself.

The company said it had been the victim of "a form of cyber-terrorism". This represents a perfect illustration of the confusion that surrounds a term that is both chillingly precise and impossibly vague. After all, what sort of terrorist group – ISIS, Peru's Shining Path, or a cadre of paranoid survivalists from Nebraska – would seek to bring horror and havoc to the world by knacker a betting shop?

For the past few years cyber-terrorism has featured prominently in the rhetoric of Western governments and security agencies. In Australia, just last month, former ASIO head David Irvine warned that jihadi groups could be preparing to take their tactics online.

"We must anticipate, given the sophistication that they have already demonstrated in using the internet for propaganda and other reasons, that they could well develop destructive attack capabilities in the near future," he told an audience in Canberra.

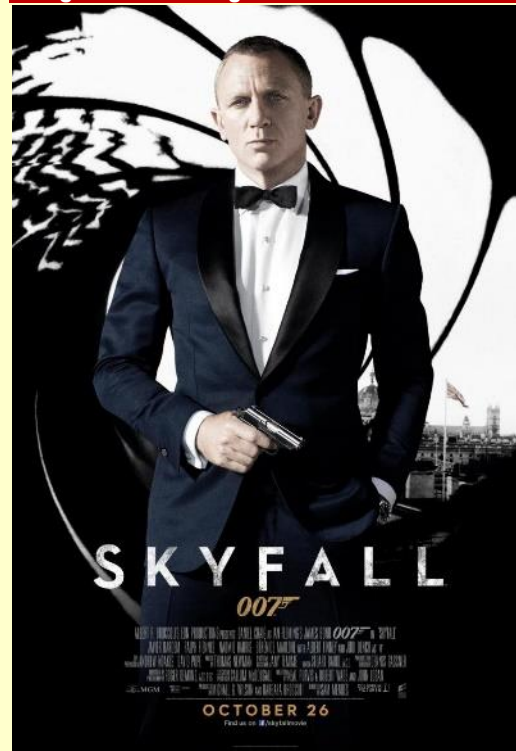
The curious thing, however, is that to date no one seems able to conclusively identify a single significant cyber attack carried out by a known terrorist group that caused real-world damage. This is in stark contrast to disruptive incursions by nation-state security agencies, organised crime groups, suspected corporate players, and political activists, of which there have been many.

"My opinion is that it's a bit of an over-used and abused term," said Julian Fay, head of South Melbourne Internet security firm Senetas.

Terrorism, he said, in the conventional sense, implies a physical act intended to cause fear

and panic among a large group of people. "We haven't yet really to date seen attacks of that nature, which would cause mass panic and terror on a scale that would be equivalent, say, to blowing up a bus in London or something like that," he said.

But no one in the business of analyzing online threats conclusively discounts the possibility that a terrorist group might one day develop the resources and skills needed to, say, cripple a nuclear reactor or bring down banking networks.



However, most suggest that the idea of bad guys destroying infrastructure with just a mouse owes more to movies such as *Skyfall* and *Die Hard 4* than reality.

The problem, though, is that in the murky environment of an anonymizing web populated by spooks, criminals, and ideological fanatics it is often very difficult to tell who is doing what.

In April this year, French television network TV5Monde suffered a devastating cyber attack that knocked out all 12 of its channels, plus its web and Facebook sites. In place of normal programming, jihadist



CBRNE-TERRORISM NEWSLETTER – December 2015

messages were broadcast. Responsibility was claimed by a group called Cyber Caliphate, on behalf of ISIS.

"That to me was concerning," said Dr Tobias Feakin, senior analyst and director of the International Cyber Policy Centre at the Australian Strategic Policy Institute (ASPI) in Canberra.

"It was very sophisticated and there was a degree of social engineering going on – to find out passwords, gain access, deliver malware, and so on. But what we subsequently found out was that it actually came from Russian sources. It kind of lowered our understanding of where their capability had got to."

David Irvine's comments were made at the launch of a paper co-authored by Feakin and released by ASPI. The [paper, *Cyber Maturity in the Asia Pacific Region*](#), rates the online defences of 20 countries. It also notes an increase in online attacks in the past year from both nation-state and non-state sources.

In terms of the latter, terror-causing intent lags well behind ability. Feakin observed that the August dump by ISIS of details about 1400 people, including Australian defense personnel, could have been compiled just by Google searching. He refused to call it cyber terrorism. He hates the term.

draconian powers in terms of content control. You have to be careful with the use of the term itself because at an international level it begins to stir up all sorts of reactions."

And, it must be said, senior Australian government ministers, even at the height of Tony Abbott's regular terrorist invocations, have been careful to avoid using it. The discourse has been couched in subtler phrases – cyber security, cyber attacks – although commentators have been left to run with it without correction.

Nor is the term used explicitly in Australia's security legislation. This possibly means, following Feakin's link between it and draconian regimes, that our own anti-terror law is less ferocious than some critics have suggested.

For one of the country's leading terrorism legal experts, however, it is still a cause for concern. Applying Feakin's draconian equivalence might thus provide some reassurance. For one of the country's leading terrorism legal experts, however, it is a cause for concern.

"It's a tricky question," said Dr Keiren Hardy, a research fellow at the University of NSW, specializing in counter-terrorism law. "I guess if you asked it of a lawyer we would say there is



OPERATION: TITSTORM
A PART OF OPERATION INTERNET FREEDOM

THE ATTACK!

1. On February 10th 8:00 AM Australian time we will begin a DDoS of government servers
2. This will be quickly followed by a shitstorm of porn email, fax spam, black faxes, and prank phone calls to government offices (emails/faxes should focus on small-breasted porn, cartoon porn, and female ejaculation, the 3 types banned so far)
3. Information on the targets for the shitstorm can be found here:
[HTTP://WWW.APH.GOV.AU/DPS/ADMINISTRATI/01.H7A](http://www.aph.gov.au/dps/ADMINISTRATI/01.H7A)

WHAT? WHEN?
PARTICIPATE FELLOW ANONYMOUS!

The Campaign begins...
8:00 AM, AUSTRALIAN TIME (GMT +10:00)
February 10th.

(FEBRUARY 9TH FOR U.S.A. AND CANADA.)
(5:00 EST | 4:00 CST | etc.)

TO FULLY PARTICIPATE IN THE ATTACK:

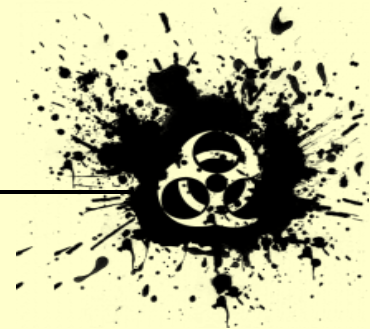
Use an IRC Client and connect to...

Server: irc.rizon.net
Channel: #titstorm

"We are Anonymous. We are legion."
Regards, Anonymous

"One thing I would say in terms of the terminology and how it's used is that certain countries are very, very keen on the use of cyber terrorism as a term," he said. "And those countries often tend to be those who have quite

no offence of cyber terrorism as such. But what we can do is look at a definition of terror under the legislation and say what use of the computer and Internet



CBRNE-TERRORISM NEWSLETTER – December 2015

technology would fit within that legislation?"

It's a critical question. A couple of years ago Dr Hardy wrote a paper on a 2010 attack mounted on several government websites by the hacktivist group, Anonymous. The action resulted in departmental home-screens being plastered with soft porn images. Anonymous called it Operation Titstorm. A repeat of the action today, Hardy said, might have severe consequences for the hackers.

"Under the Australian definition of terrorism, an act that has a political motive, that is intended to influence the government by intimidation, and which interferes with electronic systems, would fall within the definition," he said.

"Operation Titstorm" was about censorship of the Internet – there's a political motive behind that. On a slightly bigger scale maybe you could say it seriously interfered with government servers. So when you look at the elements of the definition of terrorism, I think those acts of hacktivism can fit within it."

He added that the legislation provided an exemption from prosecution for political protest, but that it had yet to be tested. Until it is, Operation Titstorm "is the type of ridiculous thing that could plausibly fall within in the definition of terrorism."

And as for real cyber-terrorism – for the Die Hard 4 super-villain taking down the electricity grid – its advent is unlikely because of the brute economics of evil.

"You can scare people by using \$500 to make an improvised explosive device," said Hardy.

"If you can behead someone on video the cost of that is negligible, but the impact, the terrorist impact, the psychological impact on the population, is enormous. So you think, is a terrorist group likely to invest two years and millions of dollars in

learning how to subtly interfere with a nuclear power station? It's easier to just go out and do something really simple."

The vast cost differential between a power station and a smartphone, however, is no reason for complacency on the part of businesses such as Internet Service Providers – the types of installation that are likely to be

the points of entry for bad guys seeking to do damage.

Indeed, for George Fong, owner of Ballarat-based boutique ISP Lateral Plains, terrorist groups might be among the many threats his business faces daily. Might be. When there's a whole bunch of bad guys shooting at you, you don't pause to figure out who's holding the guns.

"We worry about cyber threats full stop, and I think that a lot of the anxiety comes from the fact we see attacks on our system not every day, not every hour, but every minute," he said.

"It's hard to differentiate between what you might consider to be the outright issues of terrorism, and commercial terrorism in the sense of crypto-ransomware, things like that, which have been remarkably successful."

Mr Fong, who is also chairman of Internet Australia, the peak body representing internet users, described terrorism as a "silent concern" at present. He would not dismiss the possibility, however remote, that Australia might one day experience a cyber attack that would have a devastating impact in the physical world.

"It's rare, but how many times have you been inconvenienced because you've rocked up to some place and you can't pay by card?" he said.

"That disruption and distraction can be done for a variety of reasons and I think that there's a realistic concern that unless you tighten up things like networks for electricity and essential services and communication then you could be left vulnerable."

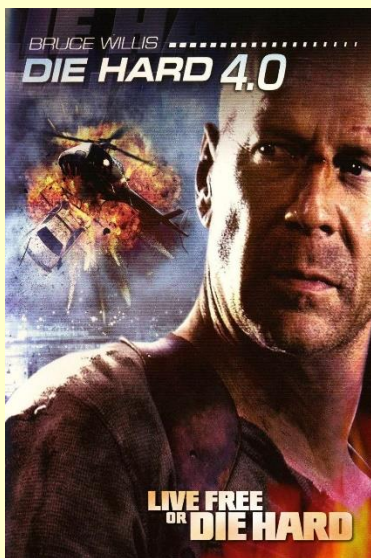
Matt Tett, who heads up Bundoora-based network security experts Enex Testlab, also saw weaknesses in the nation's civilian infrastructure.

"The bad guys have all the time in the world – they can take years to compromise a system if it's worth it," he says.

"Banks are very good at security, because any loss could potentially become a public incident.

"Other organizations nowadays are getting there, but some utilities have core critical systems, electronic systems, that are now becoming networked. Those products do not necessarily have a lot of security built into them because they were never intended to be online."

Tett said his company consulted with "around 40" state and federal government bodies about network security. "Some are well



CBRNE-TERRORISM NEWSLETTER – December 2015

coordinated; others almost take a shotgun approach."

Last week's claims that Chinese operatives have been trying to hack into three companies bidding for Australia's next submarine contract suggest that nation-state spooks might well be a bigger concern than cyber terrorists.

Some experts fear cyber incursions into Australia, from whatever source, could succeed not through lack of defensive resources, but through lack of coordination.

"One issue in Australia is that security agencies tend to be very 'siloed' – separate – so there isn't a lot of collaboration between them," says Tett. "People protect their own patch, and information is regarded as being on a need-to-know basis so is not shared around. We are several years behind other countries in this regard."

From one perspective, however, this needn't necessarily be a bad thing. In organizational terms, the fewer connections that exist between the component parts of a cyber matrix – the many systems that govern the running of a city, for instance – the more resistant it is to total failure.

"The advantage that we've got at the moment, ironically, is the complete disorganization of our communication systems," says Fong.

"The fact of the matter is that there is a lack of co-ordination on the net in terms of where things are, and a lack of agreement about how things work, that sometimes plays into our advantage. If you attack one system, you don't necessarily get access to the others."

It's a precarious basis on which to claim safety, but perhaps it also distracts from the main issue. Perhaps the evil cyber-terrorist mastermind will remain a purely celluloid creation.

"Let's be careful," said Tobias Feakin. "Cyber terrorism is a term I have issues with because it just doesn't fit. What we're concerned about is the use by terrorist groups of the online environment to progress their cause, and it's not that they are conducting terrorism via cyber means.

"It's the fact that they are using the online medium for propaganda and recruitment. And it happens at a rate of speed that governments simply can't compete with at the moment."

Hackers go on a Greek bank spree over weekend

Source: <http://en.protothema.gr/hackers-go-on-a-greek-bank-sprees-over-weekend/>



Three banks were on alert all weekend after hackers made attempts to intrude into their security systems. The National Intelligence Service, Cyber Crime Squad of Greece and Bank of Greece worked with bank officials all weekend in an attempt to stall off the hackers, who are believed to be coming from Russia, say sources. Over 30 people have been trying to get control of the banks for the last three 24-hour periods and are **seeking bitcoin for ransom** so as not to cause damages in banking transaction systems.



CBRNE-TERRORISM NEWSLETTER – December 2015

Information released by the Greek police state that the hackers go under the name Armada Collective. The deadline to receive the ransom is Monday, November 30.

Hilton hotels hit by cyber attack

Source: <http://www.terrorismwatch.org/2015/11/hilton-hotels-hit-by-cyber-attack.html>

Nov 25 – US hotel chain Hilton has revealed that hackers stole credit card information from some of its point-of-sale computer systems.

Hilton did not reveal the extent of the breach, but warned anyone who used credit cards at Hilton Worldwide hotels between November 18 and December 5 of last year or April 21 and July 27 of this year to watch for irregular activity in their accounts.



Information swiped by malicious code that infected systems included credit card holders' names along with card numbers, security codes and expiration dates, Hilton global brands executive vice president Jim Holthouser said in an online post yesterday. The hackers did not get people's addresses or personal identification numbers, according to Holthouser.

Hilton said that it is investigating the breach with the help of third-party forensics experts, law enforcement and payment card companies.

The announcement came just four days after Starwood Hotels, which operates the Sheraton and Westin chains, said that hackers had infected payment systems in some of its establishments, potentially leaking customer credit card data.

The hack occurred at a "limited number" of its hotels in North America, according to Starwood, whose other well-known chains include St Regis and W Hotels.

Starwood said that an investigation by forensic experts concluded that malware was detected in some restaurants, gift shops and other points of sale systems at hotels.

"The malware was designed to collect certain payment card information, including cardholder name, payment card number, security code and expiration date," the group said in a statement.

India to Launch World's Biggest Biometric Database

Source: <http://i-hls.com/2015/11/india-to-launch-worlds-biggest-biometric-database/>

Nov 27 – **In an effort to combat identity theft and fraud in the country, India is launching a new biometric database – the world's largest.** With over 1.25 billion citizens India has one of the world's biggest populations. The challenges presented by this ambitious project are enormous, but so are the opportunities, says MapR who were commissioned for the work by the Indian government.

Aadhaar, a 12 digit unique identifying number issued to each citizen, is to be paired with biometric identity verification procedures. To achieve this, a large database of fingerprints and iris scans is to be created. Through access to this database identity can be proven in highly reliable manner.



CBRNE-TERRORISM NEWSLETTER – December 2015

Over a hundred million identifications take place each day, and for the system to work efficiently the process must be streamlined and work without a hitch. MapR, who develop and distribute Apache



Hadoop technology that integrates enterprise storage and real-time database technology, are bringing their expertise to provide solutions to these challenges.

“Multiple challenges include storage analytics to make sure the data is accurate, security, and very high-volumes of authentications,” says John Schroeder, MapR co-founder and CEO.

The company aims for speeds of approximately 200 milliseconds per query, but that is not the only issue they face. Much of India’s population lives in rural areas still not connected to all the amenities of the 21st century.

“It had to be implemented in a very economical way,” says Schroeder, “enrollment is on inexpensive laptops, the low bandwidth and resilient technology must be able to work with the registrations coming in from areas of low connectivity.”

This new database should provide increased security for India’s large population, greatly reducing the risk of identity fraud and financial damage. It will be one of the most advanced systems of its kind in the world.

“Aadhaar is a huge leap-frog over the U.S. where social security is just a number,” says Schroeder. “we don’t have the validation and biometric identification to match the person.”

Terrorists 'could hack NHS computer systems' in threat 'only dwarfed by weapons of mass destruction'

Source: <http://www.walesonline.co.uk/news/wales-news/terrorists-could-hack-nhs-computer-10548669>

Dec 05 – Experts have warned terrorists could hold the NHS to ransom by hacking computer systems and changing patients’ records.

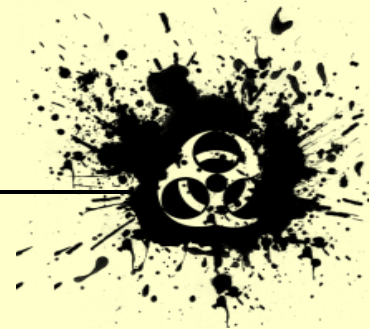
The health service is particularly sensitive because it holds so much data about the public and about employees.

Bank account details, addresses, National Insurance numbers and millions of health records are all held by the organisation.

In Wales alone 72,464 people were employed by the NHS last year.

“Outside of weapons of mass destruction it probably constitutes the most serious threat to infrastructure and services in Britain,” former Intelligence and Security Committee chairman Kim Howells said.

“The NHS and NHS records could be attacked in a number of ways.



CBRNE-TERRORISM NEWSLETTER – December 2015

If the electrical system went down nurses and doctors could not get into work.”

There could be numerous reasons to attack the NHS, the former Foreign Office minister said.

“People could hack into it for monetary gain or to get prisoners released if they were a terrorist group,” the former Pontypridd MP said.



“The NHS is a vast organisation. Parts will be properly protected – other parts will be a shambles.”

'You could kill people'

Internet security expert Professor Andrew Blyth, of the University of South Wales, said: “If someone was to attack the NHS – not just in Wales but in the UK – if that attack was successful that could have dire consequences for the UK and for people.

“You can imagine the kind of things that could be done to computer systems, things like breaking into blood banks and changing all the entries.

“Then whenever blood was given to anyone it could effectively kill them.

“So, yes, you could kill people. And, yes, there are issues around people being blackmailed.

“If someone has gone to an STD clinic, and picked up something interesting, that could be used that could be used to blackmail them.”

But accessing systems from the outside was not easy.

He feared the bigger threat could come from an insider possibly working with someone on the outside.

Prof Blyth also envisaged a Stuxnet scenario. Stuxnet was a malicious computer worm used by the US to sabotage Iran's nuclear program in 2009 and 2010. It worked by causing

systems to fail in a series of apparently unrelated events.

“But there is a big gap between something being possible and the practicalities of doing it,” Prof Blyth added.

Aberystwyth University's cyber dimension lecturer, Madeline Carr, feared data security problems were inevitable for the health service.

A hacker could break into systems to alter medical charts, she said.

“Changes to people's medication or treatment could be made to damage them or a whole bunch of people.

“It's valuable information and pretty sensitive.”

Medical records 'worth more than credit cards'

She feared criminals were already planning hacks.

“I guess there are people out there right now thinking of ways it could be exploited,” Ms Carr said.

“We are bound to see pretty disturbing breaches as we go down this path.

“We are all flying in the dark. With the best of intentions we are not going to be able to transition from the time where records were stored in paper packs without there being some pretty serious problems.”

One source close to the NHS agreed blood groups were “interesting”.

“If you want to upset people don't break into the system and steal National Insurance numbers.

“Take a blood group and change 10% of them. Then ring the chief executive and say 'I have changed 10% of your patients' blood groups. Give me a million dollars.’

“It is a hypothetical extortion attack. It could be terrorists or criminals that would do this.”

Medical records were worth a lot, the insider said.

“On the black market the cost of a credit card is maybe a dollar or two dollars.

“The cost of a medical record can be \$30 to \$50. It goes for more because you can do more with the data.

“These are the kind of issues you and I would not think of because we are not criminals.

“Medical security is a fascinating area.”



National IT systems 'checked regularly'

The UK Safer Internet Centre's Andrew Williams warned people lost control of their data the moment they gave it up.

"You're trusting the organisation that you're giving that data to," he said.

"It's important for us to have faith and trust in organisations we've given our data to.

"But the reality is that there are an awful lot – TalkTalk, British Gas, Marks and Spencer – all big organisations that have shown themselves as being vulnerable to cyber attacks and hacks.

"And hacks are increasing in regularity."

The NHS were "battling the threat of hacking in line with many other organisations" he said.

NHS Wales Informatics Service are responsible for keeping data safe on this side of the border.

A spokesman said: "Like any organisation the NHS in Wales faces challenges protecting data and therefore we have a number of security controls, products, and initiatives in place to ensure that protecting patient information and the data in health care IT systems in Wales is a principal objective.

"The informatics service runs regular security checks on national IT systems, encrypts data across networks, and trains staff to be aware of the potential risks to data."

Three-Quarters of Internet Users Can't Recognize Online Threats

By Amanda Vicinanza (Senior Editor)

Source: <http://www.hstoday.us/single-article/three-quarters-of-internet-users-cant-recognize-online-threats/f5b9eb796c14b995cc340fee5c8ca67b.html>

Dec 12 – Although the devastating nature of cyber attacks has become well-known with the proliferation of serious, high profile security breaches in recent years, an overwhelming minority of Internet users possess the skills necessary to protect themselves against online threats.

According to [a new survey](#) by cybersecurity firm Kaspersky Labs and B2B International, **three-quarters of Internet users would download a potentially malicious file because they lack the cyber knowledge they need to spot dangers online. The survey quizzed 18,000 Internet users from 16 countries around the world about their online habits.**

"Consumers need to make themselves more aware of the dangers of the online world, in order to protect themselves and others," David Emm, principal security researcher at Kaspersky Lab said in a statement. "If a consumer is in a dodgy bar, they are unlikely to start counting large sums of cash, it just would not be streetwise or sensible. The same sort of instinct should come into play when consumers go online."

The respondents were asked to consider several potentially dangerous situations during common Internet uses, such as web surfing, downloading files or using social networks. Depending on the possible negative

consequences, each answer was given a certain score. The safer the user's choice, the higher their score, and vice versa.

The survey revealed that a significant number of users are unable to identify a cyber threat. Only one out of four users could identify a genuine webpage without selecting a phishing option as well. Additionally, while specifying the web pages on which they were prepared to enter their data, over half—58 percent—of users only named fake sites.

"Checking for signs of malicious activity, and knowing how to spot a phishing page or dangerous download option is vital," Emm said. "However, no matter how cyber-savvy a person is, it is unsafe to go online without putting security solutions in place. Cyber criminals are constantly developing new ways to target people and only the most up to date security software can protect users against some threats."

In addition to failing to identify online threats, Internet users also have trouble protecting their virtual information.

According to the results of the test, while choosing a password for a new account,



CBRNE-TERRORISM NEWSLETTER – December 2015

only 38 percent of respondents thought of a new and more complicated combination.

Furthermore, 14 percent of respondents risk having several accounts simultaneously compromised in the event of a data leak by using the same password on all occasions. Users also put their information at risk by choosing insecure methods for securing passwords, including writing them down on paper or saving them on a mobile phone.

These findings corroborate Kaspersky's October report, [The Compared Perceptions of Passwords and Underwear Report](#), which revealed 73 percent of surveyed users would rather reveal their passwords than go without underwear.

Commenting on the report on a recent company blog post, Kate Kochetkova said, "The problem to be focus on here is that so many users only care about security to a medium level, if they care about it at all."

Consequently, Kochetkova recommended creating unique and reliable passwords for all accounts.

"Many people are careless about their devices and the data stored on them: they enter their personal information on phishing pages, choose passwords that are too easy, follow any proposed links, download and install unchecked software ... All this makes them vulnerable and easy targets for fraudsters, criminals and tricksters," the report concluded.

Could an attack on the electric grid mean cybergeddon?

By Robert J. Samuelson

Source: https://www.washingtonpost.com/opinions/could-an-attack-on-the-electric-grid-mean-cybergeddon/2015/12/06/52371aa2-9ace-11e5-8917-653b65c809eb_story.html



The Empire State Building towers over the skyline of a blackout-darkened New York City in 2003. (George Widman/Associated Press)

Dec 06 – When it comes to cyberwar and cyberterrorism, we need to think the unthinkable, says veteran TV journalist Ted Koppel. And for Koppel, the unthinkable is this: Someone hacks into the nation's electric power grid and causes large parts of it to crash for a prolonged period.

Anyone who has endured a blackout from a storm or mechanical breakdown — probably most Americans — knows how frustrating and infuriating it can be. You lose your lights, refrigeration, communications and sense of control. But two certitudes limit the anger and anxiety: First, outages are usually small

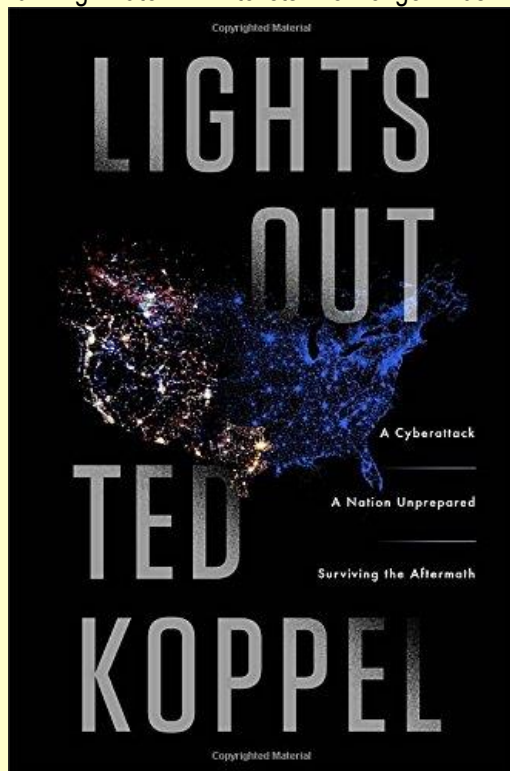
geographically; and second, we know that power will be restored in days or weeks.

Not so with a cyberattack, which aims to cripple the system and cause chaos. Lengthy disruptions may be widespread. Then the effects become horrific, as Koppel writes in his new book, ["Lights Out."](#)

Darkness descends on cities and suburbs. As refrigeration fades, food inventories are exhausted. Resupply is difficult, because — among other reasons — "gas stations without backup generators are unable to operate their pumps." Water supplies are



also paralyzed by inert pumps. “There is little running water . . . toilets no longer flush.”



Routine payments, being mostly electronic transfers, are virtually impossible. People feel increasingly isolated and vulnerable.

There are emergency plans, Koppel writes, for natural disasters and electrical outages “of a few days” but no plan for many millions losing electricity “for months.” Once people realize they’re “on their own,” there’s a “contagion of panic.” The likelihood of looting is obvious.

The Internet, whatever its advantages, has become a potential “weapon of mass destruction,” Koppel argues. Without the frightening label, I have made the same point in recent [columns](#).

Let’s concede: We may exaggerate the danger. Cybergeddon may not be inevitable. There’s a long history of false alarmism. In the 1950s, people feared thermonuclear war. At the turn of the century, the Y2K computer bug allegedly threatened havoc. After 9/11, there were widespread warnings of terrorism using chemical or biological agents, as well as a “dirty” nuclear bomb. More recently there was an Ebola scare. As yet, none of these predicted calamities has occurred.

Some self-restraint may be built into the system. It’s likely, experts tell Koppel, that both the Chinese and Russian governments have penetrated vital U.S. cybernetworks, but they may be deterred from mounting destructive

attacks for fear of retaliation. The United States, said one general, has the world’s best “cyber offense” — the ability to damage other countries’ networks — but a weak defense. Highly networked countries may refrain from mutual destruction.

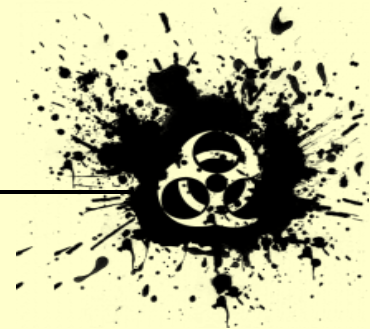
Still, Koppel has an easy time building a case for worry. When he asks Janet Napolitano, former secretary of homeland security, the chances that some adversary will knock out a significant part of the power grid, she responds, “Very high — 80 percent, 90 percent.” More troubling: Koppel cites George Cotter, a former chief scientist at the National Security Agency, who has repeatedly contended that the grid is dangerously porous to hostile intrusions.

What especially bothers Cotter is the deregulation and restructuring of the electric utility industry. Traditionally, the industry was dominated by a small number of large companies responsible for generating, transporting and delivering power to customers. But in recent decades, these various functions (generation, transportation and delivery) have been split among separate firms. Cybersecurity becomes harder, because the task of protecting the grid is spread among many more businesses.

To be fair, Koppel quotes utility executives as asserting that the grid is highly resilient. Taking down the grid, said one manager, “is not nearly as simple as I think some people . . . believe.” It’s hard for outsiders to referee these technical disputes. But we should not assume that the self-restraint of major countries will keep us safe. We’re also vulnerable to rogue states (think North Korea or Iran) and groups of terrorists and anarchists. The Internet empowers the weak: The thought of an Islamic State hacker probing for openings in European and U.S. networks is chilling.

So far, hacking has involved mostly commercial and criminal misdeeds. These are costly and inconvenient. But they are a lesser danger. The real threat is hacking intended to destabilize entire societies. Along with the grid, communications and financial networks pose similar dangers. There are limits to how much we can protect ourselves, but any improvement requires a change in consciousness.

There’s a conflict — largely ignored — between exploiting all the Internet’s economic opportunities and reducing its threats to social peace. “There is



CBRNE-TERRORISM NEWSLETTER – December 2015

not yet widespread recognition,” writes Koppel, “that we have entered a new age in which we are profoundly vulnerable in ways we have never known before.” That’s our dilemma. The

more functions we put on the Internet, the more dependent on it we become. And today’s dependency is tomorrow’s vulnerability.

Robert J. Samuelson writes a weekly economics column that usually runs in The Post on Mondays. He was a columnist for Newsweek magazine from 1984 to 2011. He began his journalism career as a reporter on The Post business desk, from 1969 to 1973. He was an economics reporter and columnist for National Journal magazine from 1976 to 1984 — when he joined Newsweek. Samuelson is the author of “[The Great Inflation and Its Aftermath: The Past and Future of American Affluence](#)” (2008) and “[The Good Life and Its Discontents](#)” (1995).

Hack Me: A Geopolitical Analysis of the Government Use of Surveillance Software

By Adam McNeil

Source: <http://www.infosecurity-magazine.com/opinions/hack-me-a-geopolitical-analysis/>

In summer 2015 a South Korean intelligence officer identified only as Lim was found alone on a mountain road, slumped over in his car. Beside his body was a piece of burnt coal that had emitted a



fatal dose of carbon monoxide poison, next to a three-page suicide note. Lim had reportedly succumbed to the pressure surrounding his work to implement controversial tracking software within the South Korean National Intelligence Service (NIS). The note suggests that as Lim lay in the car, one Italian company was clearly on his mind: **Hacking Team.**

A few days earlier, in a major twist of irony, Milan-based Hacking Team was itself hacked. More than 400GB of internal data was extracted by unknown perpetrators, who then gleefully used the organization’s own Twitter account to break the news. For those outside the industry, Hacking Team—made up of a small group of sophisticated hackers and programmers—exists to develop customized malware that gathers intelligence against desired targets. They market their services to entities around the

world, who then deploy the software against their own adversaries.

Security researchers and journalists alike have been combing the data to identify the technical methodologies adopted by this secretive organization. Vulnerabilities have been [discovered](#) and quickly integrated into well-known exploit kits. Microsoft was forced to deploy an out-of-band update to address the memory corruption of an Adobe kernel module. Mozilla temporarily blocked Adobe Flash until significant patches could be released.

The bigger picture is even more worrisome. The organization’s customers allegedly include nations such as the US and Italy, but there are also reports of sales to those with questionable human rights records and/or countries that may engage in political oppression.

Lim’s suicide note points to this murkiness. Addressing the NIS agency director, the vice director, and the bureau chief, he said: “My excessive ambition at work

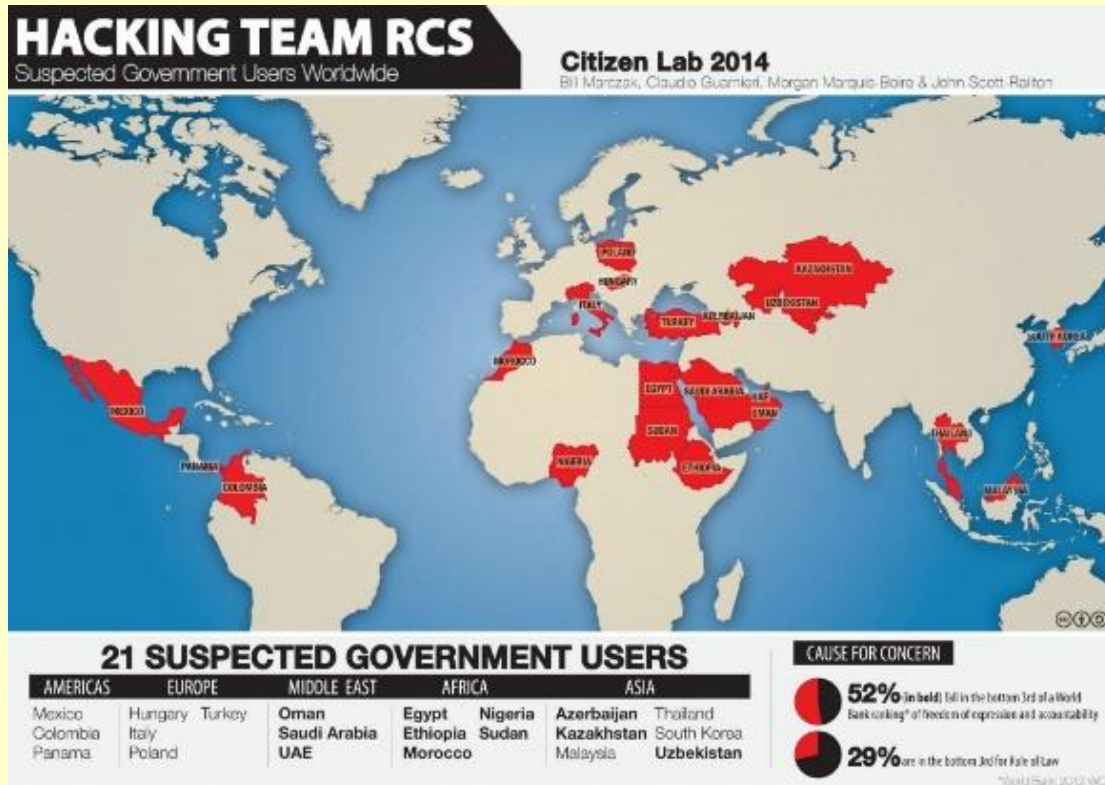


CBRNE-TERRORISM NEWSLETTER – December 2015

appears to have caused today's situation." Lim was [reportedly](#) responsible for purchasing and implementing the Hacking Team's surveillance software, Remote Control System, for use against the country's North Korean neighbors. Official accounts indicate that the note maintains the technology was never used against domestic targets; however, the NIS is currently the subject of what South Korean officials call a 'field investigation' for allegations that similar technology was used to spy on the public ahead of the 2012 presidential election.

together in clusters to overpower larger areas, say an entire city, to monitor the communications of an expanded pool. *The nature of the design dictates that all communications within the powering vicinity of the device are and analyzed—everyone falls within the net, not just the designated targets.*

Public awareness of the Harris StingRay II product emerged in 2011 when [reports](#) first surfaced of an 'off the grid hacker' named Daniel Rigmaiden. In 2008, having been charged with tax fraud, Rigmaiden walked into



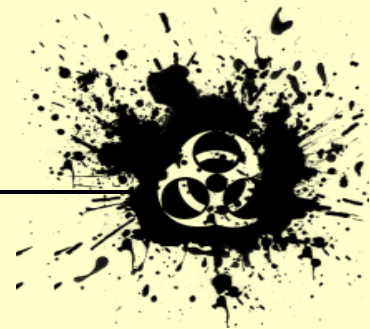
Players in the Game

In 2008, while financial markets were imploding, companies within the surveillance industry were seeing their revenues soar. Hacking Team and Gamma International were still developing their spy-tool infrastructure, but Florida-based defense contractor Harris Corp. was already marketing its second-generation IMSI-catcher known as the StingRay II to U.S. law enforcement and federal agencies.

IMSI-catchers are often [small-suitcase-sized devices](#) that mimic legitimate cellphone relay towers. The devices are designed to overpower legitimate cell towers, forcing cellphones in the area to relay information that can be used to locate a subject of interest. IMSI-catchers can be deployed to home in on suspects known to reside in a small area, or can be grouped

a lawyer's office complaining of 'government rays being sent into his living room.' No one was willing to hear his case, so Rigmaiden decided to defend himself. He spent years gathering formal transcripts and documents from local meetings to glean possible insights into the technology responsible for putting him behind bars.

After [reportedly](#) analyzing over 15,000 documents pertaining to various cell technologies and devices, Rigmaiden finally discovered references to new 'investigative techniques' that—through the use of FOIA requests and the assistance of the ACLU and EFF—helped shed light on the elusive technology that was being marketed to federal and state agencies. Rigmaiden eventually lost his Fourth Amendment



challenge to the use of the StingRay device, but the public debate regarding the use of such technologies had just started.

Sting in the Tale

To prevent discovery of such products' capabilities, their developers can use the power of contract law and non-disclosure agreements (NDAs) to maintain strict confidentiality with its clients. These restrictions are often so stringent that they mandate the withholding of information from official documents and even other government officials. And of course, they prevent federal and state officials from disclosing any information, [or even the existence](#), of the StingRay system.

Here's how this plays out in the real world. In one Florida case, a man facing a near-guarantee of four years in prison for armed robbery saw his sentence reduced to six months' probation through a plea bargain. That was after prosecutors were ordered to disclose information surrounding the use of the StingRay device to opposing attorneys. In other reports, St. Louis prosecutors dropped a total of 14 charges against four men accused of first-degree robbery and other crimes. All charges were dropped when the officer involved was scheduled to give a deposition regarding the techniques used during the investigation.

There's no end to the irony here. The NDA requirements of the very products marketed to protect citizens from crime essentially allowed accused criminals and intruders to go free because the contract prevented the disclosure of information regarding the products used to get the evidence. [Despite public discourse](#) and loud objections from the likes of the ACLU and EFF, law enforcement agencies are not alone in using surveillance tools to monitor large swaths of the population. Many governments are doing the same thing.

Tortured justification

On 14 July, Hacking Team CEO David Vincenzetti released a statement on the [company website](#) detailing the attack on its systems while attempting to sway public opinion regarding the exposed tactics. First, he promoted the "comprehensive," "easy to use" and "powerful" surveillance capabilities of the company's product line, then validated the actions of his company by pointing out that the

company only sells the product to approved government entities. Keep in mind, the information released through the Hacking Team data dump demonstrates that countries are spending millions to thwart attacks against their infrastructure, and are using the very same tools against their adversaries. Vincenzetti went on to list some former clients: Russia, Ethiopia and Sudan.

Several days later, Chief Marketing and Communications Officer Eric Rabe released a follow-up statement in which he claimed that "there is only one violation of law in this entire episode, and that one is the criminal attack on Hacking Team."

Coincidentally, the day after Hacking Team released its initial statement about the hack of its internal systems, [the FBI announced the arrest of a 20-year-old FireEye intern and mobile malware researcher](#) named Morgan Culbertson, and the subsequent dismantling of the Android-based Dendroid malware toolkit, which he is accused of developing and selling on the recently shuttered Darkode marketplace. While details are still awaited, initial reports indicate that Culbertson only developed and sold the malware toolkit to interested parties, and may have had no plans to use it himself. Basically, he wrote a piece of malware and sold it to those who wanted it, *just like Hacking Team*.

The Dendroid malware is an Android-based package that allows its owners to gather personal information—visited websites, keystrokes pressed, passwords, etc. Known as Remote Access Trojans (RATs), these programs have been around for years; familiar names include Poison Ivy, Back Orifice and Sub7. Most RATs are similar in that they allow for the harvesting of usernames and passwords via keystroke collection capabilities, and possess mechanisms to allow it to go undetected from anti-virus programs.

Future Ethical Concerns

Given the nature of international terrorism, some can justifiably see these tools as necessary weapons of war, but that's a gross over-simplification. Unlike, say, surgical strikes with guided missiles, unpatched exploits can affect all computer users regardless of country, origin or intent. If zero-day exploits are to be compared to machines used by the armed forces, then they



need similar restraints and definitions, something akin to a weapon of mass destruction.

That brings us back to the suicide of the South Korean official, which prompted this investigation. His was surely not the only tragedy; there have likely been many abuses enabled by the use of these technologies by oppressive governments. That's why it's time to create a new roadmap to the future. These digital innovations are by nature secretive, and so are many of the institutions using them. But does the security industry have a duty to consider the customer base for these tools?

So why is Hacking Team, which develops and sells malware to oppressive nations, better than an individual who develops and sells malware to unsavory online characters? If anything, the purchase, sale, and use of zero-day exploits poses far greater dangers than an individual marketing an Android-based malware toolkit. This is the core of the ethical concerns plaguing this field. Activities illegal in one country may be legal in another, and most digital advances don't respect geographic boundaries any way.

On July 21, just two weeks after the Hacking Team breach, a mysterious Reddit post

appeared under the [/r/hacking](#) board claiming to be interested in starting a new company with a similar agenda to Hacking Team. The [Reddit post](#), which was active for less than 24 hours, stated: "Creating a hacking team. Must have at least a basic understanding. Add Leo Da Vinci on line, with an android phone if interested."

Obligations

The battle is raging. Organizations that develop and market the use of government-only surveillance tools will continue to grow and thrive—and so will those attempting to expose the secrets of such groups—along with those that want to exploit the technology for nefarious purposes.

The use of zero-day exploits by commercial entities for financial gain is also a dangerous practice that potentially jeopardizes everyone. If companies that use exploits to compromise targets of national interest come to learn that other, less savory individuals are using the same exploits for illicit purposes, do they have an obligation to disclose the problem?

Maybe the next big data dump will give us the answer.

Adam McNeil is a Malware Intelligence Analyst, Malwarebytes Labs.

A Look at 2015: Cyber-Threats Show Evolution and Growth

Source: <http://www.infosecurity-magazine.com/news/a-look-at-2015-cyberthreats-show/>

Cyber-threats have grown worldwide over the course of the past year, showing both tactical evolution, greater sophistication and a few significant new trends.

Geographically speaking, Kaspersky Lab has noted especially strong growth in detected threats in African countries, including Nigeria.

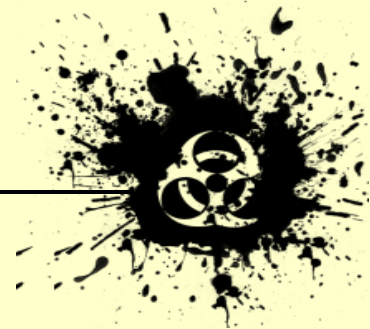
"The continued increase in threats and cybersecurity matters certainly shows that African countries are a growing target for cybercrime, and as a result, countries like Nigeria need to pay attention to this reality and the future trends and predictions in this space," said Dirk Kollberg, senior security researcher, Global Research and Analysis Team (GReAT), [Kaspersky Lab](#).

This dovetails with overriding trends in 2015 globally. The growing number of attacks, the numbers of both attackers and their victims, together with a greater focus on cyber-security

in defense budgets, new or enhanced cyber-laws, international agreements and new standards have all redefined the rules of the game.

GReAT [described](#) cyber-activity as "elusive" going into 2015: Full of cyber-criminals who are proving hard to catch, cyber-espionage actors who are even harder to attribute, and with privacy often the most elusive of all. That has proven to have come to fruition.

There has, for instance been an evolution of malware techniques to support better cyber-espionage. In 2015, GReAT [discovered](#) previously unseen methods used by the Equation group, whose malware can modify the firmware of hard drives, and by [Dugu 2.0](#), whose infections make no changes to the disk or system settings, leaving almost no traces in the system. These two cyber-



CBRNE-TERRORISM NEWSLETTER – December 2015

espionage campaigns surpassed anything known to date in terms of complexity and the sophistication of techniques.

Also, 2015 saw the merger of cybercrime and advanced persistent threats (APTs). In 2015 the [Carbanak](#) cyber-criminal gang stole up to \$1 billion from financial institutions worldwide using targeted attack methods.

2015 also marked the advent of wars between APTs. In 2015, Kaspersky Lab recorded a rare and unusual example of one cybercriminal attacking another. In 2014, [Hellsing](#), a small and technically unremarkable cyberespionage group targeting mostly government and diplomatic organizations in Asia, was subjected to a spear-phishing attack by another threat actor, [Naikon](#), and decided to strike back. Kaspersky Lab believes that this could mark the emergence of a new trend in criminal cyber-activity.

Overall, the picture that emerges is one of escalation and tactical evolution on the part of the bad guys.

Cyber Predictions for 2016

By Joe O'Halloran

Source: <http://www.infosecurity-magazine.com/news-features/predictions-for-2016/>

The association of Charles Dickens with Christmas is more or less indelible. And as the holiday period begins, the words of the great author seem rather appropriate if not altogether apposite as one, as one tends to do at this time of year, looks back at the events of 2015 in the world of Infosecurity. But it is not to *A Christmas Carol* that we should consider, but instead to *A Tale of Two Cities* and its very famous opening. To wit: "It was the best of times, it was the worst of times, it was the age of wisdom, it was the age of foolishness, it was the epoch of belief, it was the epoch of incredulity, it was the season of light, it was the season of darkness."

It was a bit of a year wasn't it? There was certainly a lot of light, darkness and incredulity. It was a year when it seemed that there was a significant breach almost every week.

A year when [Talk Talk](#) transformed itself from being a mere leading telco to being a case study in how not to do it when it comes to reacting to a security breach. A year when everyone, much to the shock and horror of the rather discreet membership, got to know about

"Select any economic sector at random, and the chances are high that you'll find something in the media about a cyber-security incident or problem," Kollberg added. "The same goes for all aspects of everyday life. This year's cyber-events have resulted in a sharp increase in interest, not only in the world's media but also in the entertainment industry. Movies and television programs featuring cyber-security issues sometimes resulted in experts appearing as themselves."

However, in addition to the positive changes of increased public awareness of risk and how to avoid it, 2015 also resulted in some negative outcomes.

"Unfortunately, for many, cybersecurity has become linked to terrorism," Kollberg said. "Today, attacking and defending internal and external networks, such as the Internet, are subjects of considerable interest to various illegal groups."



[Ashley Madison](#). A year when [Chrysler](#) had to respond to the news that control of its Jeeps, including steering, could be taken over by hackers exploiting holes in the in-car entertainment system. A year when the [US Office of Personnel Management \(OPM\)](#) revealed that highly sensitive background-check data on 21.5 million individuals had been stolen in a successful attack on its systems.

A year when the battle between privacy and state data access was as hot as ever, with [the UK government passing a bill immediately denounced as a snooper's charter](#). A year when the [internet of things](#) was transformed into a new, widespread attack surface. Oh and a year when security industry 'legend' John McAfee returned from exile with a spring in his step, announcing new technology, denouncing old enemies and even revealing a potential run for the US presidency next year.

But despite all of the above, it was also a year that the security industry can be proud of. It was



CBRNE-TERRORISM NEWSLETTER – December 2015

also the year when cyber-security leapt out of the laboratory and IT bunker and into not only the boardroom but also the mainstream. In fact 2015 witnessed the launch of two prime-time TV series, [CSI Cyber](#) and [Mr. Robot](#). Everyone now knows about IT security and hopefully armed with such knowledge people at work or at home will engage with it in a more robust manner.

The [UK government even committed £1.9 billion to cybersecurity](#) over the course of the

current parliament including a National Cyber Centre designed to act as a single point of contact to simplify and strengthen government effort on cybersecurity and improve engagement with industry.

So the future looks bright for 2016 as government, business and public alike join the battle against cyber-criminals, hackers and state actors. But, and a really big but, the work will never end: the sheer amount, variety and innovation in attacks will see to that.

Joe O'Halloran is Editor & Publisher, Infosecurity Magazine.

The mind of a cyberterrorist, a neglected aspect of cybersecurity

Source: <http://www.homelandsecuritynewswire.com/dr20151217-the-mind-of-a-cyberterrorist-a-neglected-aspect-of-cybersecurity>

Dec 17 – **A new study by Max Kilger, director of Data Analytics Programs at the University of Texas at San Antonio (UTSA) College of Business, is delving into an aspect of cybersecurity rarely explored before now: the human component. Kilger's research utilizes his talents as a social psychologist to show that at the beginning of any digital threat is a real person with unique motivations.**



"I've spent a fair amount of time trying to get people to understand that the human component of cybersecurity is very important," Kilger said. "Understanding the motivations of cyberterrorists was a foreign concept until very recently and still is to many information security professionals."

UTSA reports that Kilger recently represented UTSA, which has one of the U.S. top

cybersecurity programs, at a NATO training facility in Ankara, Turkey. There, he stressed the importance of understanding that cyberterrorists are different from traditional terrorists. There are several motivations for the attacks they carry out. Kilger said that while some are driven by ego, politics or entertainment, the most common reason is money.

"You can basically rob a bank without actually robbing a bank," he said. "The risk of getting caught is fairly low and the chance of success is pretty high."

Kilger is among the UTSA faculty leading the study of the human component of cyberterrorism.

The reason why this topic is lesser known, he said, is that security professionals become very focused on the technological side of responding to attacks and lack the social psychology background to analyze and understand the human being on the other side of

that attack.

"Being able to project future scenarios is one of the most important aspects of cybersecurity," he said. "A lot of information security efforts are defense-based and reactive. We need a more proactive approach." According to Kilger, a new approach is needed because now a single person can effectively



attack a nation-state. In his study, published in *IEEE Explore Digital Library*, he explains that the dramatic shift in power between a country and an individual is very enticing and it is one sign that a cyber terrorism community could be on the rise.

“As a social psychologist, you look at markers and clues. You analyze what’s happened before and how that informs what’s going on now,” he said. “Losses are adding up significantly. They’re recruiting all the time and they’re very organized.”

As societies become more reliant on the Internet the threat of cyber terrorism looms larger. It is something Kilger said needs to be kept in mind moving forward in a world where cars and airplanes are connected to the Internet.

“There’s no easy solution,” he said. “We need more understanding of why these attacks occur and why people do them. Then we can start figuring out what their targets will be and what they’re likely to do. With that, we can stop them from happening.”

— Read more in Max Kilger, “Integrating Human Behavior Into the Development of Future Cyberterrorism Scenarios,” paper presented at the [10th International Conference on Availability, Reliability and Security \(ARES\), Toulouse, France, 24-28 August 2015](#); published in [IEEE Explore Digital Library \(Fall 2015\)](#)

Terrorists used encrypted apps to plan, coordinate Paris attacks

Source: <http://www.homelandsecuritynewswire.com/dr20151218-terrorists-used-encrypted-apps-to-plan-coordinate-paris-attacks>

Dec 18 – The leaders of U.S. and European law enforcement and intelligence agencies have been explicit in their warnings: commercially available communication devices equipped with end-to-end encryption software make it impossible for security services to track terrorists plotting an attack – or monitor the terrorists’ communication while the attack is under way; “FBI unable to break 109 encrypted messages Texas terror attack suspect sent ahead of attack,” [HSNW, 11 December 2015](#); “Privacy vs. security debate intensifies as more companies offer end-to-end-encryption,” [HSNW, 9 July 2015](#)).

FBI director James Comey last week told lawmakers that one of the suspects in the foiled terror attack in Garland, Texas, in May 2015 had exchanged 109 messages with sources in a “terrorist location” overseas ahead of the attack. U.S. intelligence and law enforcement agencies, however, have not been able to break into and read those messages because they were exchanged on devices equipped with end-to-end encryption software.

Was the Garland attacker receiving instructions from his handlers, and, if so, who were they and what were their instructions? If the Garland attacker was a member of a terrorist cell, were these handlers relaying messages to other cell members? Was the attack part of a larger plot

to attack several targets simultaneously, as would be the case in Paris on 13 November?

The FBI was already monitoring those sources in a “terrorist location,” so they had the assume that the 109 messages coming from Texas during the run-up to the Garland attack were not innocent messages about family matters or an upcoming basketball game. Yet, the end-to-end encryption made it impossible to break into these messages, learn the details of the terrorist attack about to be carried out, and do something to prevent it from taking place. In the aftermath of the attack – when there was no longer any doubt that the Texas messages sender was a terrorist planning to kill Americans – the end-to-end encryption makes it impossible to learn more about the scope and nature of the terrorist’s support network, in the United States and abroad, thus making it impossible for the security services to dismantle it.

Even if a court were to issue a warrant allowing the FBI to break into the messages, the device maker and service provider would not be able to comply: With end-to-end encryption devices, the manufacturer and service provider do not have the key to decrypt the messages – there is no back door. Leaders of law enforcement and intelligence service argue that without such a back door,



terrorists – and criminals – have achieved immunity from tracking and monitoring. The Internet has become a “haven for terrorists,” the director of Britain’s MI5 bitterly complained. Officials familiar with the investigation into the 13 November Paris attacks have told CNN that the Islamist militants who perpetrated the attacks used encrypted apps to hide details of their plan. CNN noted that this is the first time investigators have confirmed encrypted messaging apps were used to plot the attacks. *Stars and Stripes* reports that officials said that WhatsApp and Telegram were amongst the apps the terrorists used before and during the attacks.

Both apps use end-to-end encryption to keep users’ conversations, images, video, and audio messages private. There have been numerous reports that ISIS terrorists are using Telegram encrypted messaging.

Pavel Durov, the creator of Telegram, has said that following the Paris terrorist attacks, his company has blocked dozens of accounts associated with the jihadist Islamic State group. In the immediate aftermath of the attacks, officials had confirmed they had found encrypted apps installed on the mobile phones recovered from the attack scenes, but would not confirm whether the apps had been used to plan the attacks.

Sources close to the investigation have now confirmed the terrorists used the encrypted messengers to communicate for a period before the attacks. What was said in those encrypted messages, and who sent and received these messages, may never be known, sources told CNN.

Earlier this year Prime Minister David Cameron spoke out about the danger inherent in allowing the use of end-to-end encryption.

“In our country, do we want to allow a means of communication between people which we cannot read?” he asked.

“My answer to that question is: ‘No, we must not’.

“We have always been able, on the authority of the Home Secretary, to sign a warrant and intercept a phone call, a mobile phone call or other media communications.

“But the question we must ask ourselves is whether, as technology develops, we are content to leave a safe space — a new means of communication — for terrorists to communicate with each other.”

The sources close to the Paris investigation say that the attackers also used a number of devices with unencrypted communication software. These attackers, however, were conscious of police surveillance and regularly changed the SIM cards in their phones to evade detection.

In his comments last week to a terrorism conference at New York Police Department headquarters, Comey said that “the use of encryption is at the center of terrorist trade craft.”

The number of technology companies offering end-to-end encryption has risen following the revelations of Edward Snowden about the NSA’s phone metadata collection program. These companies have so far resisted calls to create back doors in their software which would allow law enforcement agencies to read encrypted communication after receiving a warrant from a court.



San Bernardino doctor was first responder to massacre

By Dr. Sanjay Gupta (CNN)

Source: <http://edition.cnn.com/2015/12/03/health/san-bernardino-swat-doctor-profile/index.html>

Before the local SWAT team arrived on the scene of the San Bernardino shooting massacre, Dr. Michael Neeki was already there, arriving just minutes after the shooting began.

"The call came in on the radio: There's an active shooter scenario in San Bernardino," said Neeki, an emergency room doctor at Arrowhead Regional Medical Center's trauma center in Rialto, California. "I just hop in the car with my tactical equipment and go to the scene. Often I don't have time to notify anybody, I just go."

Pulling up in front of the Inland Regional Center, Neeki immediately began suiting up in his military boots, helmet and Kevlar vest, and checked his assault rifle, eerily similar to the one being used by the shooters. Without waiting for the rest of his SWAT team, he grabbed his medical pack and headed into the unknown.



San Bernardino shooting: Inside the ER 02:45

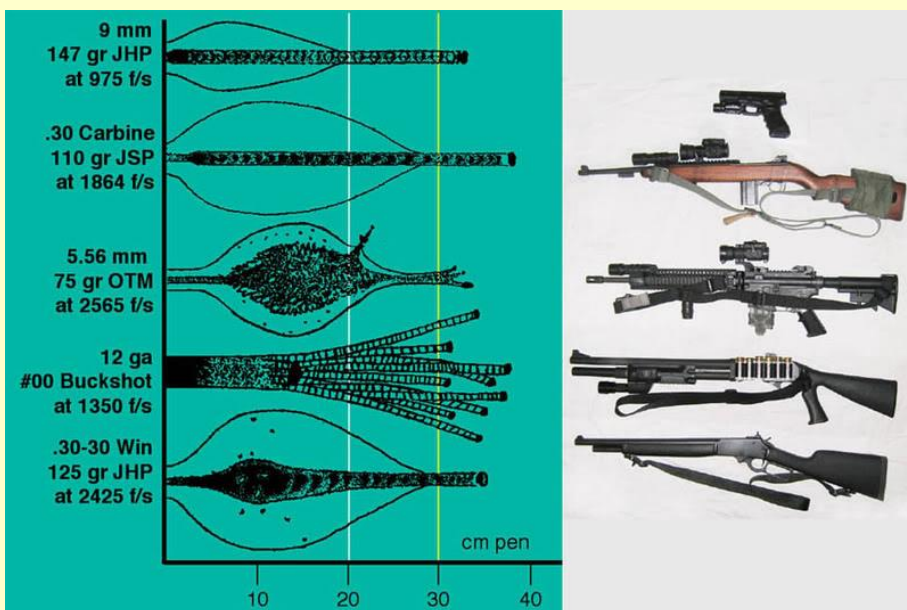
"At the time that you go in it is still an active situation, so you don't know what you will encounter," Neeki said. "It was one of the most organized scenes I had ever seen but you

could feel that energy of worry. They [police on the scene] were worried if the shooters were [still] in the building and are they going to hurt more victims."

Unfortunately, on this day 21 people were wounded, and 14 people died. "There were a lot of head injuries, chest injuries, and they didn't have a good chance of surviving," Neeki said. "We are very sad. There is no good news when you find out that your fellow citizens have died for no good reason."

A new kind of doctor

Neeki is a new kind of doctor, a hybrid of healer and soldier, an increasingly necessary type of medic trained to be able to defend as well as save lives.



As assault rifles have replaced handguns as the weapon of choice in gang, street and mass shootings, the injuries and treatment needs have changed.

"So, we are now going to this assault rifle injury-type pattern which rips and shreds apart organs in your body, tissues in the body, vessels as they're going through," Neeki explained. "So you have to be ready to put in a tourniquet to avoid the bleeding, or quickly staple a wound in the field.

Or use an Israeli bandage, which is a

compression dressing. I also have a clotting factor you could put in a lesion."



CBRNE-TERRORISM NEWSLETTER – December 2015

If this sounds like battlefield medicine, that's because it is. Neeki said much of what doctors know today about treating assault rifle wounds has come from the wars in Iraq and Afghanistan. And because



wounds like these shorten survival time for victims, it also means physicians need to be on the scene immediately, just like medics in foreign combat zones.



Haemostatic gauge



Chest seal



Modern tourniquet

EDITOR'S COMMENT: Three valuable assets both in war and "peace"



Urban battlefield

Putting medics into U.S. urban combat zones is a relatively recent phenomenon. The Bureau of Alcohol, Tobacco, Firearms and Explosives started putting paramedics in the field after the deadly shooting at the Branch Davidian compound in February 1993. Now in the second decade of the program, the bureau has about 70 special agents embedded with their special response teams.

Another recent shift in law enforcement tactics has been to put officers in emergency medical training. But critics worry they may not develop enough skills to function as well as a fully trained medical practitioner. Thus the notion of training medical professionals to become soldiers.



CBRNE-TERRORISM NEWSLETTER – December 2015**Doctor, protect thyself**

"Shooters ready?" yells the sergeant. "Yes sir!" comes the chorus of voices from the men in the training room. "Then move!" he barks. "Threat!" The assault rifles blaze. "Threat!"

With each sound-off, the men advance, aiming another blast of ammo at the targets on the wall. Neeki



is one of them, training the day after the massacre next to his SWAT team brothers.

"I don't want to get hurt," said Neeki. "If someone has the intention like yesterday of coming in and just indiscriminately shooting and I'm the first there, I want to be able to defend myself and those civilians. A good guy should be able to defend himself and also help everybody else."

Neeki, 51, is familiar with self-defense, having been born in Iran and drafted into the Iraqi war at age 18. But after 27 years in his adopted country, he didn't expect his combat experience would be needed here.

"Never in a million years, but now that I'm here, this is one of my duties," said Neeki. "It's a privilege to work here and it's a privilege to be a part of this team, to serve the community out there. It's the least I could do."

EDITOR'S COMMENT: AK-47 is the rifle of choice of both criminals and terrorists worldwide. Assault rifles produce wounds seldomly seen by most urban surgeons and emergency medicine personnel. In that respect further training need to be implemented. On the other hand waiting for the incident to be stabilized or end might cost lives (it happened in many occasions). Here the main problem is to persuade civilian medical first responders to proceed to such specialized training and expose themselves to same dangers as their police counterparts. We have the same problem in CBRNe operations. Ambulance crews usually prefer to stay in the "Cold Zone" resisting any interference to both "Hot" and "Warm" zones. This was one of our major problems during 2004 Olympic Games in Athens. And this was the main reason that the Greek military was involved in the Games by creating one specialized hospital-based unit (my Hospital CBRN Response Unit at Army General Hospital of Athens) and a second unit in support of emergency personnel deployed in the Hot/Warm Zones. Eleven years after 2004, local medical community still refuses to be involved in operations other than those in a safe environment. If we do not adjust our medical interventions in urban combat zones people might die because of our delay in provision of medical services on site.

Training on Response to Active Shooters

Source: <http://www.dhs.gov/science-and-technology/st-supports-nypd-active-shooter-exercise>

After months of coordination between the Department of Homeland Security (DHS) Science and Technology Directorate (S&T) and the New York Police Department (NYPD) Counter Terrorism Division, the NYPD conducted an active shooter training exercise on November 22. The exercise not only tested their training and proficiency, but also allowed them to incorporate several commercial technologies that could benefit future emergency situations.

"Not only was I impressed with the quality of the training and the level of proficiency displayed, but also with the coordination and unity of effort of the event," said S&T's Deputy Under-Secretary for Science and Technology Dr. Robert Griffin. "I am really pleased that

DHS S&T had the opportunity to help support this important mission, playing a critical role in working with our partners in NYC."

During the active shooter exercise, Griffin was joined by Homeland Secretary Jeh Johnson in NYC Mayor Bill de Blasio, Police Commissioner William Bratton, and Fire Commissioner Daniel Nigro.

S&T's Homeland Security Advanced Research Projects Agency (HSARPA) Explosive Division team worked hand-in-hand with the NYPD Counter Terrorism Division to help fund, develop the concept for, provide training in advance, and showcase technologies for use in future emergencies. The exercise scenario, included a suicide

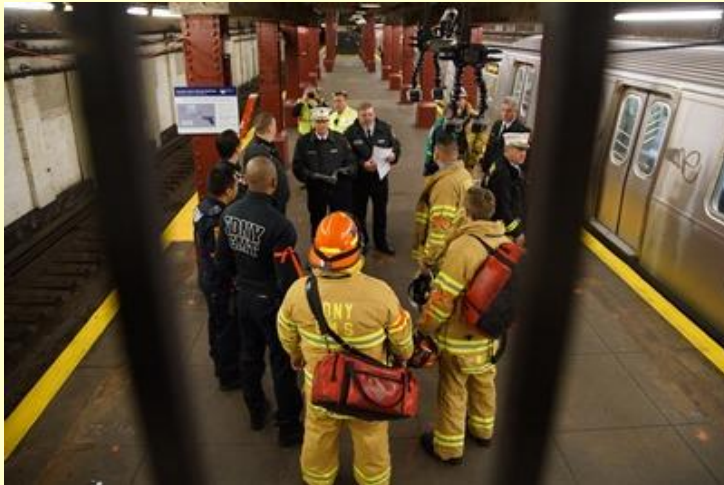


CBRNE-TERRORISM NEWSLETTER – December 2015

bomber and two active shooters, and took place at a closed in New York City (NYC) subway station. The event drew participation from numerous local and federal agencies, including DHS headquarters, S&T, the U.S. Army's Armament, Research Development and Engineering Center (ARDEC), NPPD, Secret Service, FEMA, the Federal Bureau of Investigation and numerous state and local agencies.

"This an extraordinary event, one that is very important to recognize because exercises and training like this improves coordination between agencies, awareness of training, and further unifies our efforts to secure our nation," Griffin, a former firefighter, explained.

The NYPD initially approached S&T more than



11 months ago and asked for support specifying the exercise should be held in a subway station. With a broad mission to deliver effective and innovative insight, methods and solutions for the critical needs of the Homeland Security Enterprise (HSE), sometimes S&T doesn't need to create new technologies or training; they can leverage resources from other federal departments. S&T's HSARPA team, which focuses on cutting-edge research to produce revolutionary

changes in technologies, new capabilities and threat and risk assessments for the HSE, S&T used its liaisons in the [Counter Terrorism Technology Evaluation Center](#) to spearhead this particular effort. The CTTEC was developed via an Interagency Agreement with ARDEC to assist in evaluating tactics, technologies, and procedures responders use when responding to an active shooter incident. S&T's CTTEC and ARDEC normally support at least two of these active shooter types of exercises annually. In August 2015, they completed an active shooter/IED exercise with West Orange New Jersey.

This is the fifth such exercise DHS has planned and coordinated to support technologies demonstrations and evaluations.

This active shooter exercise afforded DHS and S&T the opportunity to observe police officers using several tools of potential value to DHS and other HSE components including an indoor shot detection capability, a geo-referenced graph for better situational awareness, and an interoperable communications capability currently used by the U.S. Army.

The exercise was specifically designed to test the coordination between multiple NYPD responder resources, Bratton was quoted as saying. He was very clear in telling citizens of New York City, that they are very well prepared and continually improving that preparedness.

While this exercise wasn't in response to the attacks in Paris, Griffin echoed Johnson when he said it should give the citizens of NYC, and the rest of the nation, confidence that all levels of the government are working together to be prepared for whatever the future may bring.

"We will continue to be vigilant and use training and preparedness events like this to improve our community's ability to respond to disasters," Griffin concluded.



Food for Thought: Emergency Shelters & Food Allergies

By Andrew Roszak

Source:http://www.domesticpreparedness.com/Medical_Response/Public_Health/Food_for_Thought%3a_a_Emergency_Shelters_%26_Food_Allergies/

Dec 05 – As many as 15 million people in the United States have a food allergy, including nearly 1 out of 13 children under the age of 18. This represents approximately [2 percent of adults and 5 percent of children](#) in the United States. According to a study released in 2013 by the Centers for



CBRNE-TERRORISM NEWSLETTER – December 2015

Disease Control and Prevention, food allergies in children [increased](#) approximately 18 percent between 1997 and 2007. Odds are that, during a large-scale emergency, people with food allergies will show up at shelters. In 2006, about [88 percent of schools](#) had one or more students with a food allergy, which can range in severity, from mild to downright deadly. **The U.S. Food and Drug Administration (FDA) estimates that anaphylactic food reactions cause approximately 30,000 emergency room visits, 2,000 hospitalizations, and 150 deaths per year.**

Given the severity of some food allergy reactions, it is certainly important to develop and implement strategies designed to limit exposures to allergens and contaminants. When examining the food allergy spectrum, more than 160 foods can cause food allergies. **However, eight major food allergens – milk, eggs, peanuts, tree nuts, soy, wheat, fish, and shellfish – account for 90 percent of all food-related reactions.** These eight food allergens are the focus of the Food Allergen Labeling and Consumer Protection Act of 2004, which requires food manufacturers to list the ingredients of prepared foods and disclose whether their products contain any of these top allergens.

Simple Steps to Reduce Food Allergy Emergencies in Shelters

No cure for food allergies currently exists, so treatments can only ease the symptoms of a food-induced allergic reaction. As a



MREs were first introduced for U.S. military use in 1981, they have undergone a series of changes, including adding ingredient and nutritional information to the packaging. MREs are a common choice to feed large groups during emergencies, since they have a long shelf life and are relatively easy to store.

According to the popular World Grocer website, there are currently about [24 MRE meal menus](#) available, of which 20 contain meat products, 2 are vegetarian, and 2 are vegan. Different manufacturers can produce these meal menus, which means the actual ingredients may vary depending on the manufacturer. Therefore, it is highly recommended that people with food allergies read the ingredient and allergen statements for each ration component before consumption. The labels on all rations meet the requirements put forth by the Food Allergen Labeling and Consumer Protection Act of 2004.

result, prevention is the best strategy. When preparing food at a shelter, good hygiene and cleanliness practices are essential. Food preparation, handling, and serving techniques are important, as even trace amounts of an allergen can cause a reaction. Ensuring hands are washed and surfaces are routinely cleaned can remove most allergens from the environment.

Likewise, shelters planning to serve meals ready to eat (MREs) should be prepared to answer questions about ingredients and allergies. This is especially true in shelters where MREs are the only meal option. Since

Food Allergy Accommodations under the Americans with Disability Act

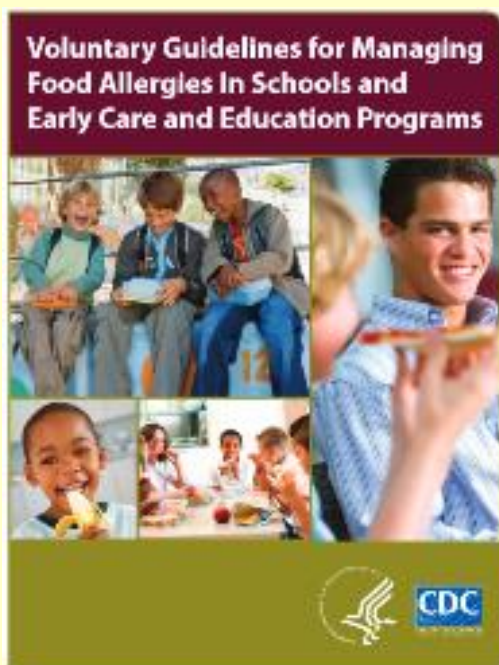
People with food allergies may require special preparations for their meals. However, these special preparations are different than accommodations required under the Americans with Disabilities Act (ADA). Although lawsuits seeking protection for food allergies under the ADA have been filed, courts have thus far been reluctant to extend ADA provisions to persons with food allergies. A disability under the ADA requires a person to have a physical or mental impairment



CBRNE-TERRORISM NEWSLETTER – December 2015

that substantially limits one or more major life activities.

Since a food allergy only manifests itself during specific times and the exposure can be managed by limiting access to the allergens, courts have found that it does not substantially limit major life activities ([Land v. Baptist Medical Center](#), 164 F.3d 423 [1999]). Similar findings have been made for people suffering from asthma and panic attacks ([Zirpel v. Toshiba America Information Systems Inc.](#), 111 F.3d 80 [1997]; [Robinson v. Global Marine Drilling Co.](#), 101 F.3d 35 [1996]). **However, shelter operators must adjust their kitchen policies in order to meet the food and beverage needs of residents and volunteers who have disability-related concerns, such as diabetics.**



Putting It All Together – What It Means for Emergency Management

Emergency management officials are faced with an enormous task and tremendous responsibility. In addition to responding to the

situation that created the need for sheltering operations, they are also charged with ensuring shelter operations are safe, accessible, and accommodating. Prolonged shelter operations necessitate the need for providing food service to those who have been displaced. Shelter plans should include guidelines for safety and sanitation procedures, especially for food preparation, service, and storage.

Appreciating that emergency shelters may be accommodating many people within a confined space, and possibly for a prolonged time adds complexity to food service issues. Staff should be trained to recognize the signs and symptoms of a food allergy incident: tingling, burning, swelling, and itching of the tongue and/or throat can be signs that a person is experiencing an allergic reaction.

Emergency planners and shelter workers are encouraged to familiarize themselves with the [Voluntary Guidelines for Managing Food Allergies in Schools and Early Care and Education Centers](#), which were developed by a multidisciplinary group of stakeholders and federal agencies, including the U.S. Department of Education and the Centers for Disease Control and Prevention. These guidelines cover a wide variety of topics that can be applied to emergency shelters, such as strategies for reducing allergic reactions and responding to life-threatening reactions.

Given the myriad of responsibilities, it is easy to surmise that many jurisdictions have not recently examined their shelter policies and procedures with a specific eye toward preventing food allergy incidents. Local environmental or health departments likely have food inspectors that can serve as a resource. The emergency necessitating the need for sheltering operations is enough to deal with, without worrying about someone having a severe allergic reaction onsite.

Andrew Roszak, JD, MPA, EMT-P, serves as the senior director for emergency preparedness at Child Care Aware of America. He is a recognized expert in emergency preparedness, public health, and environmental health. His professional service includes work: as the senior preparedness director of environmental health, pandemic preparedness, and catastrophic response at the National Association of County and City Health Officials; at the MESH Coalition and the Health and Hospital Corporation of Marion County, Indiana, as the senior preparedness advisor supporting Super Bowl 46 and the Indianapolis 500; as a senior advisor for the U.S. Department of Health and Human Services; on the Budget and HELP Committees of the United States Senate; and at the Illinois Department of Public Health. Before becoming an



attorney, he spent eight years as a firefighter, paramedic, and hazardous materials technician in the Chicago-land area. He has an AS in Paramedic Supervision, a BS in Fire Science Management, a Master of Public Administration, and a Juris Doctorate degree. He is admitted to the Illinois and District of Columbia Bars and is admitted to the Bar of the U.S. Supreme Court.

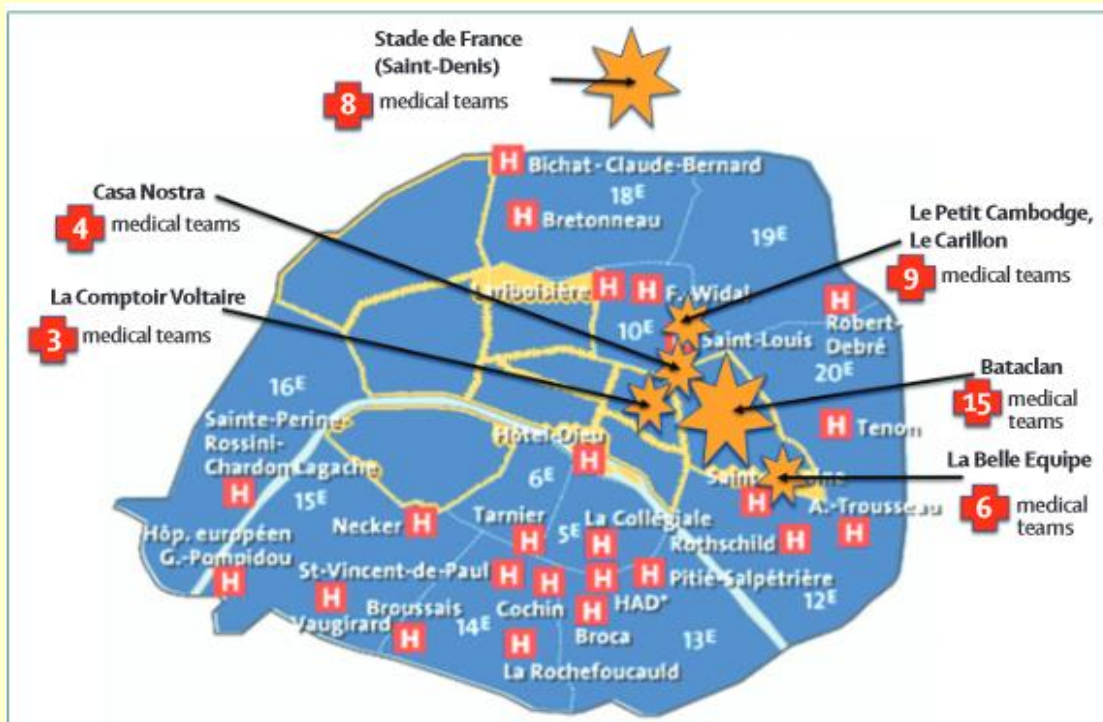
The medical response to multisite terrorist attacks in Paris

Source: <http://www.thelancet.com/pb/assets/raw/Lancet/pdfs/S0140673615010636.pdf>

The medical response to multisite terrorist attacks in Paris



Martin Hirsch, Pierre Carli, Rémy Nizard, Bruno Riou, Barouyr Baroudjian, Thierry Baubet, Vibol Chhor, Charlotte Chollet-Xemard, Nicolas Dantchev, Nadia Fleury, Jean-Paul Fontaine, Youri Yordanov, Maurice Raphael, Catherine Paugam Burtz, Antoine Lafont, on behalf of the health professionals of Assistance Publique-Hôpitaux de Paris (APHP)



EDITOR'S COMMENT: This a **must read article** proving once more that the unexpected always happens and the preparedness is better the restoring the ruins. Sincere congratulations to all medical staff doing more than their best to save lives after Paris' bloodshed!

San Bernardino Medic Had 5 Seconds to Check if Each Massacre Victim Was Alive or Dead

Source: <http://www.emergencymgmt.com/safety/San-Bernardino-medic-had-5-seconds-to-check-if-each-massacre-victim-was-alive-or-dead.html>

Dec 09 - As the water raining down from the overhead sprinklers pooled in rivers of blood and the smell of gunpowder hung in the air Wednesday, Ryan Starling remembered his



CBRNE-TERRORISM NEWSLETTER – December 2015

training. He got out his white tape. More than two dozen victims lay on the floor at the Inland Regional Center, the 33-year-old medic recalled Tuesday.

Starling began moving from body to body to determine who might survive.

"In five seconds, you look at their skin color, their breathing and you feel their pulse," he said. "By all those things, you are determining if they are critical or deceased."

He marked the dead with white tape so he and other rescuers could focus their efforts on the living.

Just minutes earlier, Starling and his SWAT teammates had been training for just such a grim task — conducting active shooter drills less than 10 miles away.

He said that when the first shooting reports arrived, his specialized team, already armed and dressed, switched out blanks for real rounds in their assault rifles and rushed to the scene.

Starling expected to be the first paramedic to arrive, and he knew that other medical personnel would be ordered to wait at a safe distance in keeping with standard policy intended to keep firefighters safe.

As a medic attached to a SWAT team,



Starling wasn't bound by that rule. He would be going in.

Coordinating with police and sheriff's deputies, the SWAT team worked first to clear civilians out the first floor of the southernmost building on the campus.

The team also searched room by room for any signs that the shooters might still be nearby.

By then, though, the assailants, Syed Rizwan Farook and Tashfeen Malik, had fled, subjects of a manhunt that would end hours later in a massive shootout.

As the SWAT team crawled slowly through the building, Starling and a fellow SWAT officer broke off from the others and approached the conference room.

He could see that a holiday party had been underway. He found the scene both grotesque and strangely ordinary. A table of pastries sat by the front door, untouched, while water rained down from the sprinklers. The carpet was soggy. He could hear voices, crying, screaming and moaning of the victims. He couldn't say how many were hurt. Perhaps more than two dozen, he thought.

Starling put aside his emotions and got to work. He needed to separate the living from the dead. He pulled on gloves and took a roll of white tape from his vest.

He moved with practiced precision, five seconds to assess skin coloring, breathing and pulse, all factors he used to determine the victim's chances for survival. He started tearing off pieces of the tape.

Fontana Police Cpl. Mike Ernes, a member of the second team into Inland Regional Center, was working in the conference room as well.

Ernes felt terrible walking past some victims to reach others who were in greater need, "one of the worst things I've ever had to experience in my career," he remembered later.

Starling started giving orders. He told police which of the wounded to take outside to the parking lot.

Joining them outside, Starling opened his medic bag, filled with medication and gauze, and directed officers to begin bandaging the victims before police cruisers ferried them to ambulances beyond the

perimeter.

San Bernardino Fire Battalion Chief Grant Hubbell had helped set up a triage site at Waterman Avenue and Park Center Drive. There, medics waited for victims.

With the wounded removed from the conference room, the SWAT team again combed the building. **When what looked like a pipe bomb was discovered**, the team evacuated until it was safe again to go back inside.



CBRNE-TERRORISM NEWSLETTER – December 2015

Soon, two suspects were spotted elsewhere driving in a black Ford Expedition.

The final shootout took place about three miles from the Inland Regional Center. San Bernardino County Sheriff's Deputy Shaun Wallen, one of the closest officers to the SUV, exchanged gunfire with Farook. As he did, San Bernardino city police Officer Nicholas Koahou got out of his vehicle to give Wallen cover and was hit in the left thigh. It felt

law enforcement to clear "hot" areas where gunmen are active.

Only an elite group of firefighters like Starling, trained to embed with SWAT teams, enter active scenes. Starling is the only medical employee in that category in the San Bernardino Fire Department, officials said. But Wednesday's shooting was an exception.

Greg Soria, a captain with the San Bernardino Fire Department, and his team decided to join



as if he had been punched in the leg. Falling to the ground, Koahou heard the gun battle rage as more than 400 shots were exchanged. Then there was silence.

Starling and his team had been called in during the shootout. Now he stood over the bodies of Farook and Malik and declared them dead. A week later, the acting deputy fire chief for the city of San Bernardino, Dan Harker, is proud of his department's response.

But the accomplishment comes with a sense of regret: Under its plan to emerge from bankruptcy, the city voted this year to disband the 137-year-old Fire Department and outsource fire services to the county. "It's a little solemn, thinking we did such a great job and now this department may go away," Harker said.

In much of the country, fire rescuers are held back in safe "cold" zones, waiting for

Starling and enter the building before it was secured. "They needed help in there," Soria said. "We went ahead and made entry."

Recommendations issued by the Federal Emergency Management Agency in 2013 call for changes so that all fire department medics, working with police, can enter "warm zones" — areas near active shooters where a threat might exist — before the attackers have been fully subdued.

"It is almost unacceptable to stand back any more," said E. Reed Smith, medical director of the Arlington County Fire Department in Virginia and an advisor on the federal government's new guidelines. "The citizen expects us to go to work."

Smith said that the proximity of San Bernardino's SWAT team, with its trained medic, resulted in



a "lucky break" that probably saved lives. U.S. Fire Administrator Ernest Mitchell, the nation's top fire official, echoed Smith's call to speed up medical responses to victims of shootings. But in an interview with the Los Angeles Times, he offered praise for the performance in San Bernardino. "I think what they did is they improvised with the tools they had available and that's great," he said.

San Bernardino Fire Capt. Mike Arviso agreed. If the medical help hadn't arrived as quickly as it did, there would have been possibly four or five more fatalities.

"Obviously we don't know," Arviso said, but having Starling near the scene "probably kept them from bleeding out." Starling thinks that more than simple luck was at play. "I believe it was divine intervention," Starling said.

Human skin detection technology improves security, search and rescue

Source: <http://www.homelandsecuritynewswire.com/dr20151211-human-skin-detection-technology-improves-security-search-and-rescue>

Dec 11 – **Color-image based systems are excellent at locating people in aerial search and rescue operations, but fall short when it comes to discerning between actual human skin and objects with similar hues.** To remedy this, researchers at the Air Force Institute of Technology (AFIT) have developed a novel two-dimensional feature space which uses the spectral absorption characteristics of melanin, hemoglobin and water to better characterize human skin.

Spectral imaging systems use information from the entire electromagnetic spectrum to provide digital images with much greater information per pixel than traditional cameras. Feature spaces in a spectral imaging system are vectors that numerically represent an object's characteristics. The skin detection approach is described this week in *Applied Optics*, a journal from The Optical Society.

The OSA reports that in their work, the AFIT **research team used feature spaces to key in on specific constituents of human tissue by using a skin index concerned with how water and melanin's presence in skin manifests at two different wavelengths in the near-infrared region. These changes would cut the overall cost of hyperspectral-based search and rescue systems by a factor of seven.**

"The study represents a crossroads between physics and statistical pattern recognition," said Michael J. Mendenhall, assistant professor, Air Force Institute of Technology, Department of Electrical and Computer Engineering, in Dayton, Ohio. "The features were designed based on an understanding of the physics behind skin's spectral shape, but in such a way

that the features separated skin and non-skin pixels in order to make the pattern recognition portion of the problem more effective."

"After a lot of investigation into spectral properties of false alarm sources, we arrived at a simple observation that skin is more red than green, due to the melanin in darker skin and oxygenated hemoglobin in lighter skin, whereas many of the false alarm sources were more green than red," Mendenhall said.

Many current image recognition programs employ hyperspectral imaging systems, which allow engineers to search for a wide variety of objects — exoplanets, oil wells, or human skin, to name a few — by looking for specific "fingerprints" in the electromagnetic spectrum. However, the involved image acquisition and post-processing are typically too slow for live search and rescue operations. Additionally, specific air platform requirements and the high cost of acquisition and management — around \$700,000 — currently puts hyperspectral systems out of reach for search and rescue organizations.

Mendenhall and his colleagues use their skin detection and false alarm suppression feature space to design an application-specific optical system using three framing cameras; their first breadboard system is about 12"x12"x6". Because their skin detection solution can be implemented with less expensive technology capable of live video frame rates, its total price tag would be around \$100,000.

OSA notes that future work for Mendenhall and his colleagues includes investigating the scattering properties of hair in order to characterize pixels as a



mix of skin and hair, as well as improving the rates of their system by accounting for skin's

specular, or mirror-like, reflection of light.

— Read more in M. Mendenhall et al., “Human skin detection in the visible and near infrared,” *Applied Optics* 54 (2015): 10559-70.

American Society of Anesthesiologists establishes new checklist for mass casualty situations to enhance emergency preparedness

Source: <https://www.asahq.org/about-asa/newsroom/news-releases/2015/12/or-mass-casualty-checklist>

Dec 07 – The American Society of Anesthesiologists (ASA) today announced the release of a new resource for hospitals, physicians and O.R. personnel – the *Operating Room Mass Casualty Management* checklist. Developed by the ASA Committee on Trauma and Emergency Preparedness (COTEP), the tool helps physician anesthesiologists and O.R. personnel optimize their response and better manage the flow of patient care during mass casualty events.

“While there has been a decrease in violent crime and gun related homicides in the United States over the past decade, mass casualty events, including mass shootings, terrorist attacks and natural disasters have increased in frequency,” said Joseph McIsaac, M.D., M.S., COTEP member and chief of trauma anesthesia at Hartford Hospital, Connecticut. “The new checklist utilizes the military planning and response principles – command, control, communications, intelligence and logistics – to prioritize tasks necessary for effective surgical and anesthetic response to mass casualty events.”

The [checklist](#) includes step-by-step instructions and outlines specific tasks that should be completed upon being alerted of a

mass casualty situation, such as ensuring adequate supplies, verifying blood availability and assigning a physician anesthesiologist as the Emergency Department liaison. While the list is guided by principles, it is meant to be customized by individual facilities to maximize management of these situations.

The committee has also updated ASA's *Manual for Anesthesia Department Organization and Management* (MADOM) by adding a new chapter on emergency preparedness in the anesthesia department. The chapter prepares hospitals and physicians for disaster response and serves as a guide for trauma anesthesia.

Disaster and emergency preparedness efforts in the public health sector are especially important in light of recent events, including the terrorist attack in France and mass shooting in San Bernadino, California. The COTEP will continue to develop tools to help physician anesthesiologists handle emergent situations and disasters including education and training for residents, practicing physicians, anesthesiologist assistants, and nurse anesthetists; creating additional checklists; and conducting research studies.



Factoring social media into crisis planning and exercising

Source: <http://www.crisis-response.com/comment/blogpost.php?post=195>

Dec 14 – When you are planning for how you're going to cope with an emergency, or when you're in any kind of exercise scenario, you're not simulating reality if you're not factoring in social media, says Lorraine Homer





Operation Strong Tower in London earlier this year also simulated the pressures of 'broadcast terrorism'

There are many different types of crisis, but few are as serious as those that occurred in Paris on November 13, 2015. This and other recent terrorist attacks have underlined that almost any organisation, any business, any venue, any event, in any country, is now possibly a target.

We're entering a new landscape where focusing efforts on protecting critical infrastructure, national events and assets is no longer enough. In Paris, it was a sports event, a concert venue, small bars and restaurants.

CEOs and operations managers in every sector should be questioning their heads of security about the state of their organisation's crisis management plan, and when it is going to be tested.

But something else Paris underlined is that the way an attack plays out is now fundamentally affected by media, and social media in particular. When the London attacks of 7/7 took place, it took time for the horror experienced by people in the tube carriages and on the bus to come out. Some of it never really has.

Andrew Neather retweeted

 **Gareth Browne**
@BrowneGareth

A hostage inside the #Bataclan writes on Facebook that they are killing people one by one #Paris #Parisattacks

 **Benjamin Cazenoves**
27 min · 🌐

Je suis encore au Bataclan. 1e étage. Blessée grave ! Qu'ils donnent au plus vite l'assaut. Il y a des survivants à l'intérieur. Ils abattent

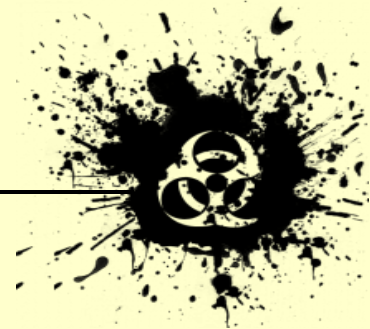
As the events in Paris unrolled, people who were trapped, injured, or held hostage inside the venues were on Twitter, Instagram and Facebook, begging for help. They posted images of helpless people dangling from windows trying to escape, and videos of gunfire and screaming, and people dragging their bleeding friends through the street.

This is a real-time climate of broadcast terrorism. It creates an irresistible pressure which challenges, changes and potentially forces the decision making of the most senior people.

This was simulated during Exercise Strong Tower, the Tier 1 counter-terrorism exercise in London in the summer (see [CRJ 11:1](#) for full report)

Whilst not the same scenario as Paris, the exercise had many common features, including a multi-site attack, use of automatic

weapons, hostage situations, and significant use of social media by eyewitnesses, hostages and victims' families.



CBRNE-TERRORISM NEWSLETTER – December 2015

The media element of the exercise used social media to apply pressure on decision-makers. The media system was on the desk of every senior player, was centre-stage at major meetings, and even drove the decision-making of Ministers at COBR.

The Metropolitan Police Service, the lead agency for the exercise, understands that social media is a game-changer. This is an organisation that can deal with more crises in a week than many organisations have to face in a year.

So it simulated what reality is now: mass use of social media, and its subsequent influence on decision-making and how it drives external factors through both its immediacy and the ability it has to change events, not just report them.

Research by Deloitte found that 1.25million smartphones are sold every fortnight in the UK. Three-quarters of adults have a smart phone; 95 per cent of them use their phones to take photos and two-thirds share these on social media sites.

This tiny piece of kit that fits in your pocket has turned everyone into a cameraman, a journalist, a broadcaster, and a network.

People are no longer reliant on traditional news channels to tell them what is news or decide what they see. They can make their own news – or more precisely, their own version of events – and they can choose what information they get, who they get it from, and who they share it with. Forget official sources. During a major incident, there are now more sources available than anyone could hope to look at in a lifetime.

This was evident in the 2013 murder of Fusilier Lee Rigby, whose killers used the smartphones of witnesses to broadcast their message, knowing full well it would be recorded and shared on social media in minutes.

It was evident in the attack at Leytonstone tube station, where a video of a comment made by a bystander created one of the most iconic phrases of 2015: “You ain’t no Muslim, bruv”, which was quickly turned into #youaintnomuslimbruv on Twitter, used more than 100,000 times over a single weekend and seen and heard by millions.

So people Tweeting “They are executing us one by one” from inside a venue changes the way an incident is handled. It also influences the perception of how an incident is being handled, something that’s critical when you are trying to reassure people and show you are in charge. And the sheer amount of unconfirmed or misinformation and the speed at which it travels will also have an impact, operationally and reputationally.

Organisations need to think again, and quickly, about their crisis management plans.

When you are planning for how you’re going to cope, or when you’re in any kind of exercise scenario, you’re not simulating reality if you’re not factoring in social media.

You might have a great exercise, but when you come to deploy your plan in real life it won’t work if you haven’t planned for the way in which social media changes these events.

You’ll be creating analogue plans for a digital event.

Lorraine Homer is the Director of Nightingale Consultants which specialises in security and crisis communication strategy and response. She was the senior communications advisor to the Metropolitan Police Service for Exercise Strong Tower.



Heated exchanges over claim of a link between global warming and terrorism

Source: <http://www.latimes.com/world/la-fg-climate-terror-20151130-story.html>



The Eiffel Tower is arrayed with special lights and messages of hope on Nov. 29, the eve of the climate change conference in Paris. (Yoan Valat / European Pressphoto Agency).

Nov 30 – **As world leaders convene in Paris this week to confront the long-term threat of global warming, the fact that their talks are taking place in a city still recovering from a deadly terrorist attack has amped up a long-running debate about how much climate change contributes to extremist violence.**

The question is playing prominently in the U.S. presidential race. The bitter disagreement it has spawned underscores the challenge climate activists' face in selling their broader message to the public.

Activists consider climate change an existential crisis that demands immediate attention. But its link to any specific occurrence, whether an individual storm or an act of terrorism, is tough to pin down. That makes the activists' case harder to sell to the public.

On the other side, conservative critics of climate activism have ridiculed suggestions that global warming is a prime security issue.

In Britain last week, Sky News aired an interview with Prince Charles in which he declared that a clear link existed between climate change and the emergence of Islamic State.

"There is very good evidence indeed that one of the major reasons for this horror in Syria was

a drought that lasted for five or six years," he said.

"Heir brained," the tabloid Sun, owned by Rupert Murdoch's News Corp, harrumphed in a front-page editorial.

Similarly heated exchanges have marked the U.S. political scene. As a result, Tom Steyer, the California billionaire who has spent tens of millions of dollars on campaigns aimed at making climate change an election issue, chose his words carefully when the question of linkage came up during a recent meeting with reporters in Washington.

But he insisted the link exists.

"It isn't us who are saying that climate matters for national security," Steyer said. "It is the CIA ... the Joint Chiefs of Staff. The national security apparatus believes that climate is a destabilizer and a creator of national-security concern. Talk to any service. The services are all over this."

Indeed, a week earlier, the CIA had made its most recent foray on the issue. The agency's director, John Brennan, told a forum in Washington that extreme weather related to global warming is exacerbating food and water



CBRNE-TERRORISM NEWSLETTER – December 2015

shortages that make populations vulnerable to extremism.

"Mankind's relationship with the natural world is aggravating these problems and is a potential source of crisis itself," he said. "Last year was the warmest on record, and this year is on track to be even warmer."

That linkage, however, was considerably more cautious than the language used by Sen. Bernie Sanders of Vermont, who said in a

to the rise of Islamic State is one [published this year by the National Academy of Sciences](#). It examined the conditions that existed in Syria in the run-up to the civil war there.

In the years leading up to the outbreak of fighting in the spring of 2011, a severe drought in the Mideast had forced the migration of 1.5 million people out of farming areas. That helped trigger civil unrest. The international



Democratic presidential debate the day after the Paris attacks that "climate change is directly related to the growth of terrorism."

Nonpartisan fact-checking groups dinged Sanders for overstating his case. They did not take issue when another candidate, former Maryland Gov. Martin O'Malley, declared that the "cascading effects" of global warming had created a humanitarian crisis in Syria that helped give rise to Islamic State.

America's intelligence agencies and armed forces have been tracking the potential effects of climate change on national security for years. Such efforts have been stepped up lately, as President Obama has increased his focus on the issue.

The risks that intelligence and military officials have identified range from instability caused by drought to the threat of naval bases being submerged by rising sea levels. The latest "Worldwide Threat Assessment of the U.S. Intelligence Community" maps out how climate change can exacerbate the spread of health-security risks such as the Ebola virus.

The report most often cited when climate activists seek to directly tie global warming

team of scientists who produced the study, led by Colin Kelley, a climatologist from UC Santa Barbara, concluded global warming had exacerbated that drought.

"We conclude that human influences on the climate system are implicated in the current Syrian conflict," the authors wrote. That's the conclusion Prince Charles appears to have been referring to.

But the study is not without critics, who note that civil war in Syria could have broken out regardless of the drought. Ethnic and religious tensions have made the country unstable for decades. Moreover, Syria's repressive government has previously faced — and crushed — rebellions. And weather was not the only culprit parching the nation's fields. Syria lacked the modern irrigation systems and agricultural infrastructure that more developed nations use to offset the effects of periodic rainfall shortages.

The back and forth over the report's conclusion highlights the political risks activists face in linking terrorism and climate change, even as the confluence



of events in Paris has the world's attention focused on the two threats in the same place. But in the backdrop of the debate are environmental groups growing increasingly frustrated with the low priority voters place on

confronting climate change. The groups are searching for messages that might more readily stir voters to action.

"We have a mission," Steyer said, "which is to prevent climate disaster."



Paris pledges, if implemented and followed, can avert severe climate change

Source: <http://www.homelandsecuritynewswire.com/dr20151130-paris-pledges-if-implemented-and-followed-can-avert-severe-climate-change>

Nov 30 – More than 190 countries are meeting in Paris this week to create a durable framework for addressing climate change and to implement a process to reduce greenhouse gases over time. A key part of this agreement would be the pledges made by individual countries to reduce their emissions.

A study published in *Science* shows that if implemented and followed by measures of equal or greater ambition, the Paris pledges have the potential to reduce the probability of the highest levels of warming, and increase the probability of limiting global warming to 2 degrees Celsius.

PNNL reports that in the lead up to the Paris meetings, countries have announced the contributions that they are willing to make to combat global climate change, based on their own national circumstances. These Intended Nationally Determined Contributions, or INDCs, take many different forms and extend through 2025 or 2030.

Examples of these commitments include the U.S. vow to reduce emissions in 2025 by 26-28 percent of 2005 levels and China's pledge to peak emissions by 2030 and increase its share of non-fossil fuels in primary energy consumption to around 20 percent. In the study, the scientists tallied up these INDCs and simulated the range of temperature outcomes the resulting emissions would bring in 2100 under different assumptions about possible emissions reductions beyond 2030.

"We wanted to know how the commitments would play out from a risk management perspective," said economist Allen Fawcett of the U.S. Environmental Protection Agency, the lead author of the study. "We analyzed not only what the commitments would achieve over the next ten to fifteen years, but also how they might lay a foundation for the future."

Although many researchers have focused on the importance of the 2 degree limit, Fawcett

and colleagues assessed uncertainty in the climate change system from an overall risk management perspective. They analyzed the full range of temperatures the INDCs might attain, and determined the odds for achieving each of those temperatures. To determine odds, they modeled the future climate hundreds of times to find the range of temperatures these various conditions produce.

"It's not just about 2 degrees," said Gokul Iyer, the study's lead scientist at the Joint Global Change Research Institute, a collaboration between the Department of Energy, Pacific Northwest National Laboratory and the University of Maryland. "It is also important to understand what the INDCs imply for the worst levels of climate change."

In the study, the scientists compare the Paris commitments to a world in which countries don't act at all or start reducing greenhouse gas emissions only in 2030.

The team found that if countries do nothing to reduce emissions, the earth has almost no chance of staying under the 2 degree limit, and it is likely that the temperature increase would exceed 4 degrees. They went on to show that the INDCs and the future abatement enabled by Paris introduce a chance of meeting the 2 degree target, and greatly reduce the chance that warming exceeds 4 degrees. The extent to which the odds are improved depends on how much emissions limits are tightened in future pledges after 2030.

"Long-term temperature outcomes critically hinge on emissions reduction efforts beyond 2030," said Iyer. "If countries implement their INDCs through 2030 and ramp up efforts beyond 2030, we'll have a much better chance of avoiding extreme warming and keeping temperature change below 2



CBRNE-TERRORISM NEWSLETTER – December 2015

degrees Celsius. It's important to know that the INDCs are a stepping stone to what we can do in the future."

To perform the analysis, the team incorporated the INDCs along with assumptions about future emissions reductions into a global, technologically detailed model of the world called the Global Change Assessment Model or GCAM that includes energy, economy, agriculture and other systems. The GCAM model produced numbers for global greenhouse gas emissions, which the team then fed into a climate model called Model for

the Assessment of Greenhouse-gas Induced Climate Change or MAGICC. Running the simulations for each scenario 600 times resulted in a range of temperatures for the year 2100, which the team converted into probabilities.

lyer said the next thing to look at is the question of the kinds of policies and institutional frameworks that could pave the way for a robust process that enables emissions reduction efforts to progressively increase over time.

— Read more in Allen A. Fawcett et al., "Can Paris pledges avert severe climate change?" *Science* (26 November 2015): 1-3

Selected Articles: Climate Change, Planetary Weapons, and Military Weather Modification. What prospects for Paris COP21?

Global Research, December 01, 2015

Source: <http://www.globalresearch.ca/selected-articles-climate-change-planetary-weapons-and-military-weather-modification-what-prospects-for-paris-cop21/5492729>

[Planetary Weapons and Military Weather Modification: Chemtrails, Atmospheric Geoengineering and Environmental Warfare](#)

By Rady Ananda, December 01 2015

Developed in 1988 by the United Nations Environment Programme and the UN's World Meteorological Organization, the Intergovernmental Panel on Climate Change (IPCC) just published [in 2013] its Fifth Assessment Report and maintains its silence on military weather modification applications which continue to skew the data.

[The Pentagon, The Climate Elephant. The US Military Machine is the World's Worst Polluter of Greenhouse Gas Emissions](#)

By Sara Flounders, December 01 2015

First published by International Action Center and Global Research in September 2014. The US military machine, is the world's biggest institutional consumer of petroleum products and the world's worst polluter of greenhouse gas emissions.

[Climate Change, Rising Levels of Greenhouse Gas Emissions and Global Warming](#)

By Jack A. Smith, December 01 2015

This article first published in December 2013, documents the failure of the Climate Change COP19 Conference in Warsaw. What prospects for Paris COP21?

[Climate Change, Geoengineering and Environmental Modification Techniques \(ENMOD\)](#)

By Prof Michel Chossudovsky, November 30 2015

Discussion of ENMOD is taboo. It is an unspoken truth. Scientists dare not address it as part of the debate on climate change. ENMOD technologies not only exist, they are fully operational. Confirmed by US military documents, a typhoon, a tsunami or an earthquake can be triggered by the use of ENMOD technologies.

[Weather Warfare: Beware the US Military's Experiments with Climatic Warfare](#)

By Prof Michel Chossudovsky, November 29 2015

'Climatic warfare' has been excluded from the agenda on climate change.





Paris UN climate change conference

Source: <http://www.consilium.europa.eu/en/meetings/international-summit/2015/11/30/>

From 30 November to 12 December, Paris hosted the 21st session of the Conference of the Parties (COP 21) to the United Nations Framework Convention on Climate Change (UNFCCC) and the 11th session of the meeting of the parties to the Kyoto Protocol (CMP 11).



On 12 December, the parties reached a new global agreement on climate change. The agreement presents a balanced outcome with an action plan to limit global warming 'well below' 2°C.

Carole Dieschbourg, Environment Minister for Luxembourg, holding the presidency of the Council, said: "Today is a day to be proud. We have agreed the first-ever legally binding and universal climate agreement which puts the world on course to avoid dangerous climate change. It is a roadmap

for a better, more just and sustainable world. The EU fought for this agreement to be as strong as possible. We have been a successful bridge builder throughout these negotiations. But let's not forget that Paris is only the beginning of a long journey. Together with all the stakeholders - NGOs, the business community and every citizen -we will now have the responsibility to translate this agreement into actions."

Donald Tusk, President of the European Council, joined 150 other leaders at the opening event on 30 November 2015. The Council formally adopted a negotiating position for the conference in September this year.

The main elements of the new Paris agreement:

- **long-term goal:** governments agreed to keep the increase in global average temperature to well below 2°C above pre-industrial levels and pursue efforts to limit it to 1.5°C
- **contributions:** before and during the Paris conference countries submitted comprehensive national climate action plans to reduce their emissions
- **ambition:** governments agreed to communicate every 5 years their contributions to set more ambitious targets
- **transparency:** they also accepted to report to each other and the public on how well they are doing to implement their targets, to ensure transparency and oversight
- **solidarity:** the EU and other developed countries will continue to support climate action to reduce emissions and build resilience to climate change impacts in developing countries



Preparing for the Unknown

By Jerome H. Kahan

Source: http://www.domesticpreparedness.com/Commentary/Viewpoint/Preparing_for_the_Unknown/

Stakeholders must be prepared for the critical implications of major natural, terrorist, and unintentional human-caused disasters. By identifying threats, dangers, and risks, then recognizing their relationships and consequences, stakeholders can build more-effective preparedness programs that leverage this knowledge of similarities and differences for various types of disaster scenarios.

“By failing to prepare, you are preparing to fail.”

—Benjamin Franklin, n.d.

“There's no harm in hoping for the best as long as you're prepared for the worst.”

—Stephen King, 1982, in “Different Seasons”

Dec 16 – Much attention has been paid to preparedness, especially since the tragic terrorist attacks of 9/11, but this concept applies to all types of disasters, not just terrorist attacks. Indeed, a disaster is considered to be an event with consequences far beyond the severity and scope of a manageable emergency, the cause of which could be high-impact attacks by terrorists, large-scale acts of nature, or significant human-caused or technologically precipitated incidents. Each of these causal agents has unique characteristics that affect preparedness needs. As defined by the Red Cross and [Red Crescent Societies](#), “Disaster preparedness refers to measures taken to prepare for and reduce the effects of disasters ... to predict and, where possible, prevent disasters, mitigate their impact on vulnerable populations, and respond to and effectively cope with their consequences.”

Threat of Terrorism

Whether located abroad or in the growing group of violent domestic extremists, terrorist actions are not predictable, but can on occasion be prevented through the difficult tasks of identifying suspects, disrupting their plans, and arresting potential perpetrators. Terrorists are relatively free to select their targets, tactics, and timing to exploit vulnerabilities, create fear, injure and kill people, destroy property, damage critical infrastructure, and contaminate food and water supplies.

As evil yet smart adversaries, terrorists can use many different types of damage-inflicting methods – including shootings, bombings, release of chemical or biological agents, hijackings, skyjackings, and cyberattacks. It is possible that a terrorist group could build a nuclear weapon by stealing such weapons if not well guarded, purchasing existing nuclear weapons on the black market, or creating relatively unsophisticated but nonetheless highly dangerous, improvised nuclear devices. Perhaps more likely than a nuclear weapon is the risk that terrorists would develop and

employ a so-called “dirty bomb” that disperses nonexplosive radiological materials – causing some injuries, requiring areas to be cordoned off, and promoting fear among citizens.

Dangers of Natural Disasters

“Mother Nature” is responsible for many natural disasters occurring in the United States – notably floods, wildfires, earthquakes, tornados, and hurricanes. However, based on historical data from past incidents, some factors can be anticipated – for example, impact areas, frequency of occurrence, type and power of destructive potential, and duration of these natural disasters.

Although natural disasters are largely unpreventable, the public can be given warnings and/or precautions can be taken before some of these incidents occur.

The potential consequences of these forces of nature are significant regarding lives lost, injuries, property damage, impact on agriculture, and economic costs; all of which differ widely as a function of population density, property values, and other



factors. Businesses exposed to these disasters may be temporarily shut down or permanently closed. Rural areas may have their crops destroyed. Entire communities may be leveled, driving residents to either rebuild or move elsewhere.

Risks of Unintentional Human-Caused Incidents

Major industrial incidents are often caused by human error or technological failure, which may result in deaths and injuries, as well as adverse economic effects. Although steps have been taken to preclude such incidents – ranging from tips to avoid household dangers to safety standards for transporting hazardous materials to codes of practice for the prevention of major industrial accidents – such events still occur. Examples include: rupture of hazardous materials in storage tanks during land or sea transport; oil pipeline breaks and drilling incidents; industrial fires; collapse of large buildings and bridges; inadvertent release of dangerous toxic and explosive chemical substances from laboratories; reactor meltdowns due to cooling system failures; and widespread water contamination from industrial runoff.

Relationships & Consequences

Interestingly, hazards are not fully independent. Natural disasters, such as hurricanes and earthquakes, can trigger damaging technological incidents. Damage and disruption from natural disasters can also open opportunities for terrorist actions as law enforcement personnel are dealing with recovery. In addition, terrorists can deliberately destroy a storage site to spread hazardous materials into populated areas.

Along these same lines, the consequences of many types of terrorist attacks may require some of the same preparedness measures as those of certain natural disasters and large-scale unintentional incidents. For example, explosive attacks by terrorists require first responder care for the injured as in the case of an unintentional industrial blast or the occurrence of an earthquake. Certain actions by terrorists, notably chemical-biological attacks, call for special preparedness measures, such as personal protective equipment for responders and also for affected citizens in the case of an inadvertent release from a hazardous material storage site. On the

other hand, natural disasters such as floods and wildfires, each creates largely unique readiness requirements that are not usually relevant either to terrorist attacks or other human-caused incidents.

FEMA at Work

The Federal Emergency Management Agency sees preparedness as the responsibility of all stakeholders in the form of a [pyramid](#), with households, neighborhoods, and communities on the lower levels and local, county, state, and federal governments at the higher levels. In this connection, FEMA has developed a five-step "[Preparedness Cycle](#)" depicting the continuous process of "planning, organizing and equipping, training, exercising, evaluating and improving," and starting all over again. In other words, any user can reach an appropriate preparedness posture by assessing threats, finding shortfalls and gaps in security measures, establishing requirements for new policies and programs, implementing these measures with associated training and exercising, reassessing the situation, and then repeating the cycle until the desired outcome is attained.

Not to ignore the need for companies to become prepared, the Department of Homeland Security (DHS), sponsors a resource called "[Ready Business](#)" to "assist businesses in developing a preparedness program by providing tools to create a plan that addresses the impact of many hazards." Although useful, this approach often leads to hundreds of different plans, since each emergency is unique and each user has different concerns.

Preparedness Guidelines

Over the years, as stated by President Barack Obama in Presidential Policy Directive 8 ([PPD-8](#)), preparedness has broadened to encompass the full range of "capabilities necessary to prevent, protect against, mitigate the effects of, respond to, and recover from those threats that pose the greatest risk to the security of the Nation." The capabilities needed to translate these five objectives into operational programs vary as a function of whether the hazard in question is terrorism, natural disasters, or unintentional human-caused incidents and also the particular stakeholder involved. How all the parts of this complex puzzle come together is explained by FEMA in



CBRNE-TERRORISM NEWSLETTER – December 2015

the National Preparedness System – a challenging and complicated guide that has unfortunately been criticized by homeland security experts as not being useful to all stakeholders, as in the 2014 *Homeland Security Affairs* article, entitled “[Preparedness Revisited: W\(h\)ither PPD-8?](#)”

Simpler preparedness guidelines should be developed for every possible user – from individuals and households to all levels of government and businesses – and for all the types of disasters these stakeholders might face.

Recognizing this need, FEMA has developed a set of preparedness recommendations about basic necessities required – for example, the availability of food, water, hygiene, clothing, radios – when facing disasters that share common features. Such an “all-hazard” preparedness plan can be adapted for specific anticipated disasters and adjusted to the needs of the locality and scale of the event, while providing at least the foundation for dealing with unexpected incidents.

This plan also needs to include psychological as well as logistical measures. The prospect of terrorist attacks, natural disasters, and

unintentional human-caused incidents bring about psychological reactions to adults and children. These reactions include depression and anxiety, with more-extreme effects tending to result from the uncertainties associated with terrorism, when other humans seek to harm

innocent people at unpredictable times and places.



Preparing for Preparedness

President Obama reminded the nation in PPD-8 that, “**Our national preparedness is the shared responsibility of all levels of government, the private and nonprofit sectors, and individual citizens.**” Yet, many agencies and organizations still have not developed emergency preparedness plans for many reasons – too busy, it will not happen here, others will take care of this, and similar excuses. Citizens have also tended to ignore the need to prepare for disasters that could impact their families and homes. This brief discussion reminds stakeholders of the need to prepare for disasters and highlights some of the important implications of terrorist attacks, natural disasters, and major human-caused incidents for their preparedness programs.

Jerome H. Kahan is an independent analyst with over 40 years of experience in national and homeland security, having held senior positions in the State Department, including the Policy Planning Staff and Counselor at the U.S. Embassy in Turkey. He has also worked with various research organizations, including senior fellow with the Brookings Institution. He has written or contributed to books and articles, taught as an adjunct professor at Georgetown University, and been a member of the Council on Foreign Relations, and the International Institute of Strategic Studies. He has a master’s degree from Columbia University in electrical engineering.

