February 2015

CBRNE NEWSLETTERRORISM

E-Journal for CBRNE & CT First Responders

10 years

www.cbrne-terrorism-newsletter.com

The Litvinenko Inquiry

By J. Millard Burr

Source: http://acdemocracy.org/the-litvinenko-inquiry/?utm_source=The+Litvenenko+Inquiry3&utm_campaign=The+Litvinenko+Inquiry&utm_medium=email

Days before the opening of the a long-anticipated public inquiry into the circumstances of the murder of former KGB spy Alexander Litvinenko, in London, the Telegraph UK reported that "American spies" of the NSA had intercepted communications between London and Moscow, fingering those involved in his murder in November 2006, which they provided to British authorities. The inquiry itself, much of which will be held in secret and will hear evidence inadmissible in a trial, is scheduled to last for two months.

© EPA

Litvinenko's murder by poisoning with a difficult to detect, rare and highly radioactive isotope, polonium-210, was described by many as a "Russian-backed" state execution. The Russians did not hesitate to use this radioactive weapon on British soil, perhaps because they knew they could get away easily.

Litvinenko sought and was granted asylum in Great Britain in May 2001. He was at the time the deputy head of the Seventh Section of the Russian FSB. Previous to the fall of the Soviet Union he had served in the ultra-secret KGB Department for the Analysis of Criminal Organizations, and after 1991 he served as a counter-terrorism expert in the Central Staff of the MB-FSK-FSB.

The Telegraph has held its own investigation and has stated that it, "unearthed an audio recording appearing to capture Litvinenko giving a detailed account of his investigations into links between Vladimir Putin and one of the world's most wanted criminals, Semion Mogilevich, rumored to head the Russian mafia that operates worldwide. The tape will reignite claims that Litvinenko could have been killed as a result of investigative work he carried out in a series of European countries after leaving Russia."

One can anticipate some startling revelations, and perhaps some clarifications of Litvinenko statements made well prior to his assassination. **Of particular interest to the author are claims the Russian did in an interview in July 2005, with the FAKT (Fact), the most popular tabloid daily in Poland, owned by the German publishing giant, Axel Springer AG.**

FAKT contacted Litvinenko after the London bombings of July 2005, and in their discussion the Russian disclosed the following:

"FAKT: Every terrorist you have named [previously in the discussion] is from 'the old staff' of the KGB. Could you name someone from recent history?

"A. Litvinenko: Certainly, here it is. The number two person in the terrorist organization al Qaeda, who they are crediting with the series of explosions in London, Ayman al-Zawahiri, is an old agent of the FSB. Being sentenced to death in Egypt for terrorism and hunted by Interpol, Ayman al-Zawahiri, in 1998, was in the territory of Dagestan, where for half a year he received special training at one of the educational bases of the FSB. After this training he was transferred to Afghanistan, where he had never been before and where, following the recommendation of his Lubyanka chiefs, he at once…penetrated the milieu of bin Laden and soon became his assistant in al Qaeda.

"FAKT: Could you hint at least, where this data [on Soviet and Russian support for terrorists] comes from?

"A. Litvinenko: I can. During my service in one of the most secret departments of the FSB, top officials from the UFSB of Dagestan, who had directly worked with Ayman al-Zawahiri…were called to Moscow and received high posts."

However, important facts Litvinenko provided on Zawahiri are demonstrably false.

With the Somalia operation winding down in 1995, bin Laden's al-Qaeda, which was then operating from the Sudan, was able to pay more attention to Chechnya and Dagestan. It funded the movement of mujahideen through Turkey to Baku, Azerbaijan, from which point al-Qaeda operatives guided mujahideen to Dagestan and Chechnya. It was an expensive proposition and was generally paid for with funds received from friends in Saudi Arabia.

The failed attempt to kill Egyptian president Hosni Mubarak during the 1995 all-Africa conference in Addis Ababa was soon found to be the handiwork of Ayman al-Zawahiri, the Egyptian exile and friend of bin Laden, then residing in Khartoum. The Sudan government cut off all funds to his Egypt Islamic Jihad, and forced his immediate exit from the Sudan. The mujahid, formerly valued and visible, was a liability that President Bashir was determined to do without. Zawahiri then began a long expedition in search of a base of operations.

Zawahiri was often on the road and, while working out of the Sudan, he had traveled with a Swiss passport, using the name Amin Othman. Consumed by perpetual fund-raising efforts to ensure EIJ's independence, he was known to have used a variety of passports to secretly visit countries…including the United States.

After his forced departure from Khartoum, he was seen in Switzerland and then Sarajevo and the Caucasus, where he hoped to set up a base of operations for his Egypt Islamic Jihad, likely in Chechnya. Crossing the border at Dagestan using a false passport he was arrested by Russian officials. As reported at the time, and apparently verified by his brother who was an al-Qaeda agent and under CIA surveillance in Albania, Ayman Zawahiri was released after six months in jail because Russian intelligence apparently failed to comprehend the importance of its prisoner.

The fact that the committed Islamist Zawahiri was coopted–whether in Dagestan or elsewhere–by Russian intelligence has never been claimed by anyone other than Litvinenko.

Most importantly, Litvinenko was greatly in error when he claimed that after his Russian training, Zawhiri "was transferred to Afghanistan, where he had never been before and where, following the recommendation of his Lubyanka chiefs, he at once…penetrated the milieu of bin Laden and soon became his assistant in al Qaeda."

Zawahiri had certainly been in Afghanistan, living there permanently in 1986. By then he had become close friends with Osama bin Laden. After the war ended in Afghanistan, Zawahiri found a home in Yemen for his Egypt Islamic Jihad, and he joined bin Laden shortly after the Saudi exile chose residence in the Sudan in 1991. His permanent residence was finally noted in Khartoum in 1993.

While the above may appear to be quibbling, one must question why an intelligence agent of Litvinenko's importance could be in error regarding the most fundamental elements of the Zawahiri biography. Anyway, this was not the reason why he was killed. He must have been provoked his former Russian employers by other statements, including this:

"FAKT: What can you say concerning the acts of terrorism in London? From what region and with what forces was this strike directed?

"A. Litvinenko: In reply to this question I can definitely say that the center of global terrorism is not in Iraq, Iran, Afghanistan or the Chechen Republic. The terrorist infection is spread worldwide from Lubyanka Square and the Kremlin cabinet."

(Retrieved from the J.R. Nyquist blog and article "A Curious Specimen," 13 August 2005.)

Whether Litvinenko will speak from the grave to prove his allegations against the Russian intelligence services remains to be seen.

***J. Millard Burr** is a Senior Fellow at the American Center for Democracy.*

IAEA chief urges vigilance against 'terrorist' nuke threats

Source: http://www.terrorismwatch.org/2015/01/iaea-chief-urges-vigilance-against.html

The head of the UN's atomic watchdog warned Monday that 'terrorists' could attack or sabotage nuclear facilities in countries where security is weak, and urged governments not to let their guard down.

"This is a very serious issue for the international community now," Yukiya Amano, director-general of the International Atomic Energy Agency (IAEA), said in a lecture in Singapore.

"In this area, international cooperation is extremely important because terrorists always target the weak link," he said.

"The country which does not recognise the threat of terrorist sabotage or attacks on nuclear power plants or facilities is the most dangerous country," he added, without referring to any specific threats or countries.

Media reports in July last year cited Iraq's United Nations ambassador Mohamed Ali Alhakim writing to UN secretary-general Ban Ki-moonabout insurgents seizing nearly 40 kilogrammes (88 pounds) of uranium compounds kept at Mosul University.

The Islamic State group has overrun parts of Syria and Iraq since last June and declared a Muslim caliphate in those areas.

Speaking to reporters later, Amano declined comment on the prospect of global powers and Iran reaching an agreement by the end of June on Tehran's nuclear programme.

"The IAEA has long been insisting that the solution needs to be found through dialogue. We welcome if and when the agreement is reached," Amano said.

"We have communications with them, we provide assistance as necessary and as appropriate, but we are not a party to this negotiation."

Iran and the so-called P5+1 group — the United States, Britain, China, France, Germany and Russia — have been seeking a comprehensive accord that would prevent it from developing a nuclear bomb in return for an easing of economic sanctions.

Iran says its nuclear programme only has civilian aims.

Videos Capture US Nuclear Physicist Offering 'Venezuelan Spy' Nuke Info

Source: http://abcnews.go.com/US/videos-capture-us-nuclear-physicist-offering-venezuelan-spy/story?id=28553152&google_editors_picks=true

New hidden camera videos made public today by the government show a former American nuclear physicist covertly meeting with a man who he believed to be a Venezuelan intelligence officer in order to sell his expertise, as well as classified information, to the South American nation.

In one from 2008, nuclear physicist Pedro Mascheroni, former scientist in the X-Division of the Los Alamos National Laboratory in the 1980s, tells the other man, who is really an undercover FBI agent, that Venezuela could test a nuclear bomb in the Pacific to put the U.S. on notice.

"Everybody sees it. You don't kill anybody. Now you tell the United States, 'Not only do we have this, but we have [these] other designs… You have to come up and say to the other nations, 'We are going to be, we're going to have an umbrella for everybody. If any nation outside Latin America attacks any nation inside Latin America, we are going to retaliate with a nuclear bomb,'" he says,

Mascheroni is a naturalized American citizen from Argentina.

In other audio recordings, referenced in court documents, Mascheroni speaks to his wife, another former worker at LANL, about his plans.

"This is very dangerous and I am doing it for money... I am, I told you, I'm not an American anymore. This is it," Mascheroni says.

Caught on Camera: Nuclear Scientist Selling Secrets; Department of Justice

In 2013 Mascheroni pleaded guilty to several of the counts involving transmitting restricted information and making false statements to federal agents. He attempted to withdraw his guilty plea last summer, but the court denied the motion. Today the Justice Department announced Mascheroni has been sentenced to 60 months in prison, followed by three years of supervised release.

"[The] defendant's aims were never noble, or part of some selfless journey that he had undertaken for the greater good of his fellow citizens," the U.S. government wrote in a sentencing memorandum in January. "Rather, his actions were criminal to their core."

In response to the government's stinging sentencing memorandum, Mascheroni's defense argued that he was something of a mad scientist "entrapped" by the government.

"Anyone who has spent time with Dr. Mascheroni knows that he is completely and hopelessly obsessed with correcting the errors he perceives in the National Laboratories' pursuit of nuclear fusion energy. This obsession has controlled his life since he lost his security clearance in 1988. Providing Dr. Mascheroni with a willing, receptive, well-funded, and non-critical audience for his scientific theories was the functional equivalent of providing crack to a cocaine addict," the defense said in a motion last week.

"We simply cannot allow people to violate their pledge to protect the classified nuclear weapons data with which they are entrusted," Assistant Attorney General for National Security John Carlin said in a DOJ release. "Today's sentencing should leave no doubt that counterespionage investigations remain one of our most powerful tools to protect national security."

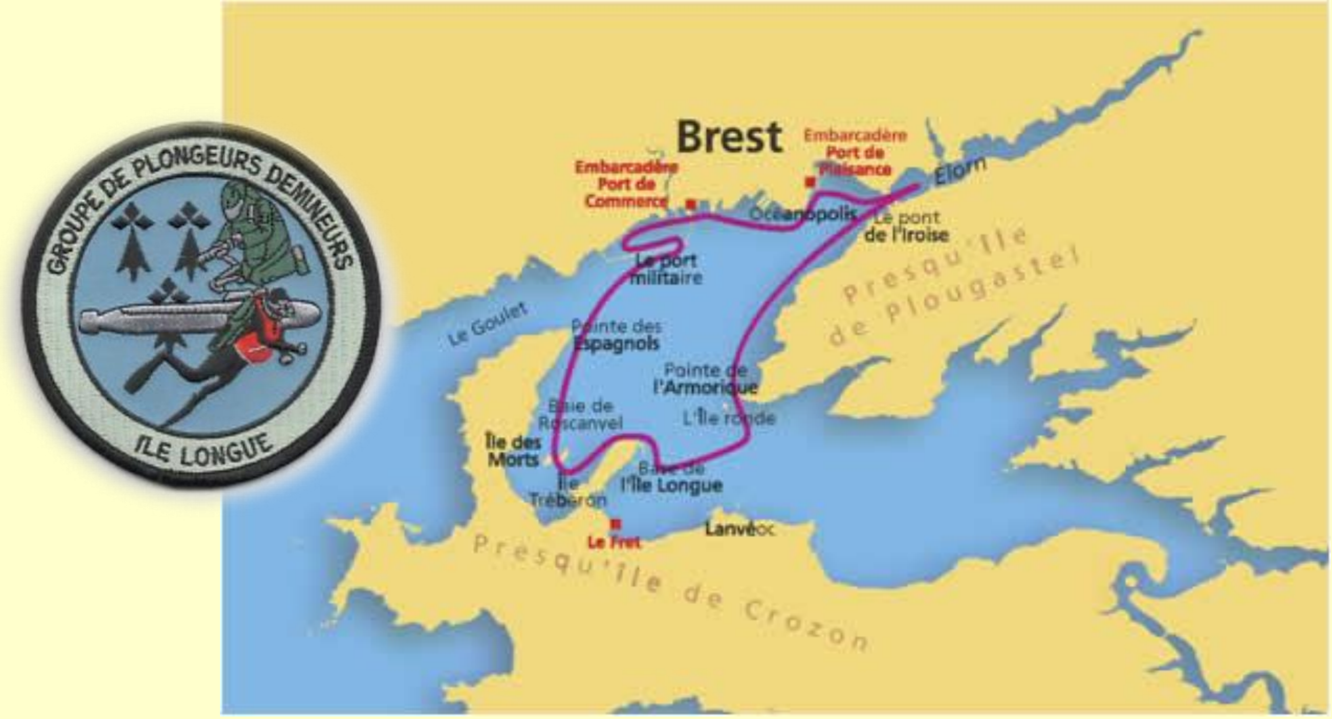
Mascheroni's wife also pleaded guilty in 2013 to conspiracy and false statements. She was sentenced last August to just over a year in prison and three years supervised release. Neither the Venezuelan government, nor any Venezuelan officials, were accused of any wrongdoing in the case.

[Editor's Note: This report has been revised to clarify that Mascheroni's statement about "doing it for the money" was made to his wife and not to the undercover federal agent, as the original version of this report implied.]

Drones spotted near the base of nuclear submarines

Source: http://www.godlikeproductions.com/forum1/message2780023/pg1

Drones have been detected in recent days near the nuclear military site Long Island in the harbor of Brest, announced Wednesday the maritime prefecture of the Atlantic, adding that these flights did not present a threat on the basis of safety.



"In recent days, drones were detected near the site of the Long Island", says the maritime prefecture in a statement. "These drone flights showed no threat characterized on plant safety," she adds.
L'Ile Longue on the Crozon Peninsula, home to four nuclear submarine ballistic missile (SSBN) of the French deterrent. This is the device and site protection teams have reported the presence of these drones in a wide area around the Forbidden basic overview.
"These detections were immediately treated by mobilizing resources and response teams provided for in this case," said the maritime prefecture.
Everything turned out drone flying over military installations subject of legal proceedings to determine the nature and origin of the overview and prosecute those responsible, given the illegal nature of these activities, said the prefecture, ensuring that the "monitor and Navy site protection ensures safety and takes into consideration the potential offered by new technologies."

Iran's Nuclear Timetable

Source: http://www.iranwatch.org/our-publications/articles-reports/irans-nuclear-timetable

Dec 02, 2014 – This report estimates how soon Iran could fuel a nuclear weapon. With its thousands of gas centrifuges, Iran now has the ability to enrich uranium to a grade suitable for use in nuclear reactors or to a higher grade suitable for use in nuclear warheads. The data below, which are based on reports from the International Atomic Energy Agency, describe Iran's uranium stockpile, its centrifuges, and the rate at which its nuclear capacity is growing.

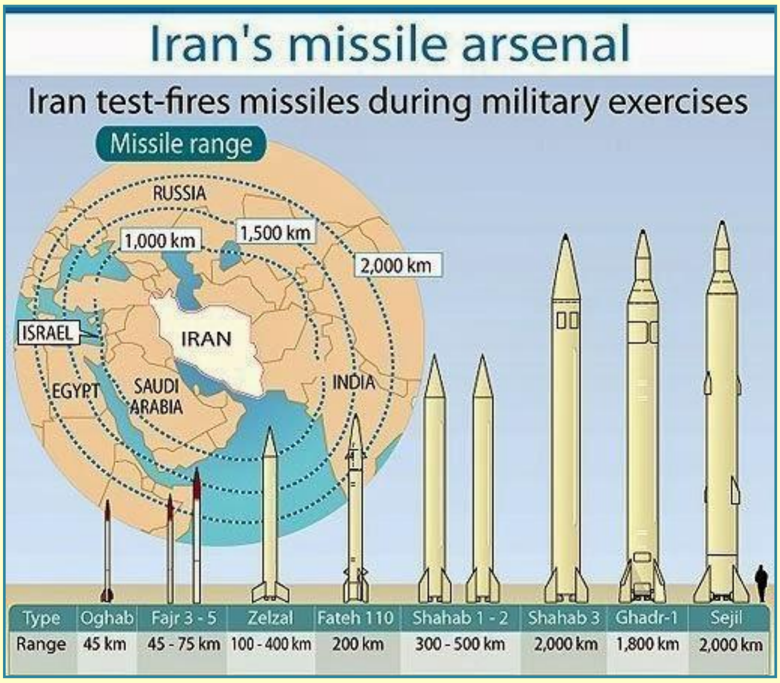
Highlights

- By using the approximately 9,000 first generation centrifuges operating at its Natanz Fuel Enrichment Plant, Iran could theoretically produce enough weapon-grade uranium to fuel a single nuclear warhead in about 1.7 months.
- Iran's more advanced IR-2m centrifuges, about 1,000 of which are installed at Natanz, would allow Iran to produce weapon-grade uranium more quickly.
- Iran's stockpile of low-enriched uranium is now sufficient, after further enrichment, to fuel approximately seven nuclear warheads.
- Because Russia has a ten-year contract to fuel Iran's only power reactor at Bushehr, Iran has no present need for enriched uranium to generate civilian nuclear energy.
- Iran could fuel approximately 25 first generation implosion bombs if it had the ability to enrich the uranium needed to supply the Bushehr reactor annually.

▶ **Read the complete article at souce's URL.**

Iran Missile Milestones: 1985-2014

Source: http://www.iranwatch.org/our-publications/weapon-program-background-report/iran-missile-milestones-1985-2014



1985: Then-speaker of the Iranian Majlis Ali Akbar Hashemi Rafsanjani leads a high-level delegation to Libya, Syria, North Korea and China, reportedly to acquire missiles.

1985: Iran receives its first Scud-Bs from Libya.

▪▪▪ ▪▪▪ ▪▪▪

January 2014: Iran's ballistic missiles are "inherently capable of delivering WMD," according to a worldwide threat assessment by the U.S. intelligence community. The intelligence community also assesses that Iran's space launch program provides the country with the means to develop longer-range missiles, including an ICBM, and that Iran maintains the largest inventory of ballistic missiles in the Middle East.

February 2014: Iran displays two satellites developed by researcher at Malek Ashtar University. "Tadbir" (Wisdom) is an improved version of the "Navid-e-Elm-o-Sanat" (The Promise of Science and Industry) satellite, with upgraded imagery resolution, while the "Khalij-e-Fars" (Persian Gulf) satellite supports secure wireless communications.

February 2014: German authorities reportedly arrest a German-Iranian man, Dr. Ali Reza B., on charges of providing Iran with components for its missile program. The equipment, worth nearly $315,000, includes dual-use items such as vacuum pumps and valves.

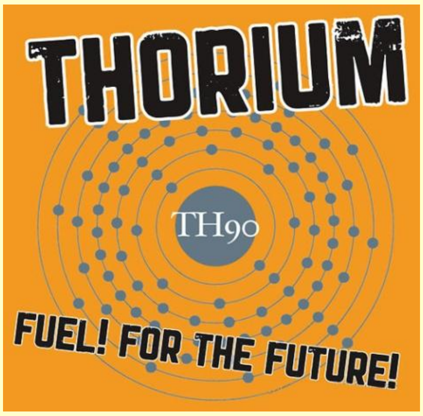
February 2014: Iran announces the test of a ballistic missile known as the "Barani." Iran claims the missile has a new submunition warhead able to better evade missile defense systems and attack multiple targets simultaneously.

March 2014: Israel intercepts a ship carrying Iranian weapons bound for Gaza. The arms seized from the Klos C, a cargo ship, include M-302 rockets, which are capable of reaching any point in Israel.

March 2014: According to a senior U.S. State Department official, Li Fangwei, a Chinese businessman indicted in 2009 for alleged sales of missile parts to Iran, remains a major supplier of Tehran's missile program. Both Li (also known as Karl Lee) and his company, LIMMT, have been sanctioned by the United States.

▶ **Read the complete article at souce's URL.**

Thorium Power Is the Safer Future of Nuclear Energy



Source: http://blogs.discovermagazine.com/crux/2015/01/16/thorium-future-nuclear-energy/#.VNNhui6TLz5

Nuclear power has long been a contentious topic. It generates huge amounts of electricity with zero carbon emissions, and thus is held up as a solution to global energy woes. But it also entails several risks, including weapons development, meltdown, and the hazards of disposing of its waste products.

But those risks and benefits all pertain to a very specific kind of nuclear energy: nuclear fission of uranium or plutonium isotopes. There's another kind of nuclear energy that's been waiting in the wings for decades – and it may just demand a recalibration of our thoughts on nuclear power.

Nuclear fission using thorium is easily within our reach, and, compared with conventional nuclear energy, the risks are considerably lower.

Thorium's Story

Ideas for using thorium have been around since the 1960s, and by 1973 there were proposals for serious, concerted research in the US. But that program fizzled to a halt only a few years later. Why? The answer is nuclear weapons. The 1960s and '70s were the height of the Cold War and weaponization was the driving force for all nuclear research. Any nuclear research that did not support the US nuclear arsenal was simply not given priority.

Conventional nuclear power using a fuel cycle involving uranium-235 and/or plutonium-239 was seen as killing two birds with one stone: reducing America's dependence on foreign oil, and creating the fuel needed for nuclear bombs. Thorium power, on the other hand, didn't have military potential. And by decreasing the need for conventional nuclear power, a potentially successful thorium program would have actually been seen as threatening to U.S. interests in the Cold War environment.

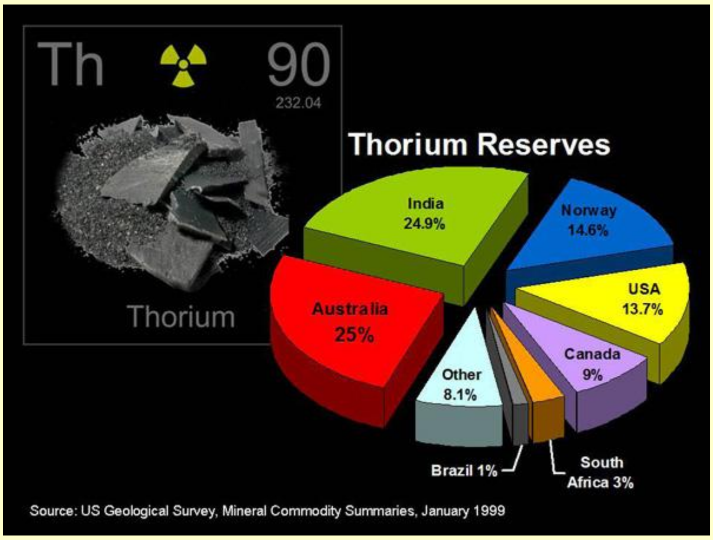
Today, however, the situation is very different. Rather than wanting to make weapons, many global leaders are worried about proliferating nuclear technology. And that has led several nations to take a closer look at thorium power generation.

How Thorium Reactors Work

The isotope of thorium that's being studied for power is called Th-232. Like uranium, Th-232 comes from rocks in the ground.

A thorium reactor would work like this: Th-232 is placed in a reactor, where it is bombarded with a beam of neutrons. In accepting a neutron from the beam, Th-232 becomes Th-233, but this heavier isotope doesn't last very long. The Th-233 decays to protactinium-233, which further decays into U-233. The U-233 remains in the reactor and, similar to current nuclear power plants, the fission of the uranium generates intense heat that can be converted to electricity.

To keep the process going, the U-233 must be created continuously by keeping the neutron-generating accelerator turned on. By contrast the neutrons that trigger U-235 fission in a conventional reactor are generated from the fuel itself. The process continues in a chain reaction and can be controlled or stopped only by inserting rods of neutron-absorbing material into the reactor core. But these control rods aren't foolproof: their operation can be affected during a reactor malfunction. This is the reason that a conventional fission reactor has the potential to start heating out of control and cause an accident. A thorium fuel cycle, by contrast, can be immediately shut down by turning off the supply of neutrons. Shutting down the fuel cycle means preventing the breeding of Th-232 into U-233. This doesn't stop the heating in the reactor immediately, but it stops it from getting worse.



Source: US Geological Survey, Mineral Commodity Summaries, January 1999

The increased safety of thorium power does not end there. Unlike the U-235 and plutonium fuel cycles, the thorium reactors can be designed to operate in a liquid state. While a conventional reactor heading to meltdown has no way to jettison the fuel to stop the fission reactions, **a thorium reactor design called LFTR** features a plug at the bottom of the reactor that will melt if the temperature of the reacting fuel climbs too high. If that happens the hot liquid would all drain out and the reaction would stop.

Powered Up

Thorium power has other attractions, too. Its production of nuclear waste would be orders of magnitude lower than conventional nuclear power, though experts disagree about exactly how much: Chinese researchers claim it's three orders of magnitude (a thousandth the amount of waste or less), while U.S. researchers say a hundredth the amount of waste.

Thorium would be easier to obtain than uranium. While uranium mines are enclosed underground and thus very dangerous for the miners, thorium is taken from open pits, and is estimated to be roughly three times as abundant as uranium in the Earth's crust.

But perhaps the most salient benefit of thorium power, in our geopolitically dicey world, is that the fuel is much harder to turn into a bomb. Thorium itself isn't fissile. The thorium fuel cycle does produce fissile material, U-233, which theoretically could be used in a bomb. But thorium would not be a very practical route to making a weapon, especially with LFTR technology. Not only would the proliferator have to steal the fissile U-233 as hot liquid from inside the reactor; they'd also be exposed to an extremely dangerous isotope, U-232, unless they had a robot to carry out the task.

Future Fuel

China has announced that its researchers will produce a fully functional thorium reactor within the next 10 years. **India**, with one of the largest thorium reserves on the planet but not much uranium, is also charging ahead. Indian researchers are planning to have a prototype thorium reactor operational early next year, though the reactor's output will be only about a quarter of the output of a typical new nuclear plant in the west. **Norway** is currently in the midst of a four-year test of using thorium fuel rods in existing nuclear reactors.

Other nations with active thorium research programs include the United Kingdom, Canada, Germany, Japan, and Israel.

There are some drawbacks to thorium fuel cycles, but they are highly technical. For instance, thorium reactors have been criticized as potentially having more neutron leak compared with conventional reactors. More neutron leak means more shielding and other protection is needed for workers at the power plant. And as in most types of alternative energy, thorium power faces a lack of funding for research and of financial incentives for power companies to switch over.

In recent decades, stories about safe, green nuclear power in popular media have tended to focus on the quest for nuclear fusion. Certainly, we can expect, and should hope, for continued progress toward that type of power. But while that happens, the investments by China, India, and other countries suggest that thorium is *en route* to contribute to the grid in the near term – and to dramatically improve the world’s energy sustainability in the process.

NTI – United Arab Emirates

Source: http://www.nti.org/country-profiles/united-arab-emirates/

The United Arab Emirates (UAE) is a member in good standing of all of the relevant nonproliferation treaties, organizations, and regimes, and is not known to possess programs for the development of nuclear, chemical, or biological weapons, or their delivery systems. Currently pursuing a peaceful nuclear program, the UAE is often referred to as a model for nuclear newcomers.

In addition to subscribing to the major nonproliferation treaties and regimes, the UAE has pledged support to a number of ad hoc initiatives, including the U.S.-led Proliferation Security Initiative (PSI). [1] Most significantly for proponents of nonproliferation, the UAE made the unprecedented commitment in its April 2008 "White Paper" announcing its intention to evaluate peaceful nuclear energy and in subsequent October 2009 domestic legislation to permanently forego the acquisition of uranium enrichment and plutonium reprocessing capabilities. [2] This pre-existing domestic commitment by the UAE is also reflected in its 2009 "123" nuclear cooperation agreement with the United States, whose language concerning no enrichment and reprocessing is often referred to in the U.S. policy community as the nonproliferation "Gold Standard." The UAE has financially supported, in the amount of U.S. $10 million, efforts to develop an IAEA fuel bank. [3] Concerned about the ambiguous nature of Iran's nuclear program, the UAE relies for its security on close strategic partnerships with the United States and France. [4] The UAE has also purchased advanced conventional weaponry, such as missile defense systems, from its Westerns partners.

Nuclear

The UAE became a non-nuclear weapon state party to the Treaty on the Non-Proliferation of Nuclear Weapons (NPT) in 1995, concluding a safeguards agreement with the International Atomic Agency (IAEA) in 2003 and an IAEA Additional Protocol in 2010. [5] In April 2008, the UAE released a policy document outlining its interest in developing a nuclear power program. [6] At the time, the country's electricity demand was growing approximately 9% annually, and at that rate the UAE would require an additional 40 gigawatts installed capacity to meet demand by 2020, though the global economic crisis has subsequently depressed demand projections. [7] Although the country is rich in natural resources such as natural gas and oil, the government argues that "known volumes of natural gas that could be made available to the nation's electricity sector would be insufficient to meet future demand." [8] The UAE concluded that nuclear power is an "environmentally promising and commercially competitive" source that could contribute to the country's "economy and future energy security," and rapidly moved forward with plans to build its first nuclear power plants. [9] In 2009, the UAE signed a $20.4 billion dollar deal with the ROK's Korea Electric Power Corporation to construct four APR-1400 reactors, with the first scheduled to become operational in 2017 and the three subsequent reactors completed by 2020. [10] On 17 July 2012, the UAE nuclear regulator, the Federal Authority for Nuclear Regulation, approved a license for construction to begin immediately on the first two nuclear reactors at the Barakah power plant near Abu Dhabi. Work on the second reactor began in May 2013. [11] The UAE has announced that it plans to build 16 reactors total. [12]

The U.S.-UAE 123 nuclear cooperation agreement entered into force in December 2009, providing the necessary legal basis for any future nuclear commerce between the two countries. The agreement had significant precedent-setting potential; if the

United States government treats future 123 negotiations similarly, nuclear newcomers could be required to accept the nonproliferation "gold standard" of forgoing enrichment and reprocessing capabilities in order to conclude a nuclear cooperation agreement with the United States. [13] However, as referenced in the "Agreed Minute," should the U.S. negotiate a 123 agreement with another country in the Middle East with more favorable terms, the U.S.-UAE agreement can be renegotiated. [14] An intense debate over whether to insist on the "Gold Standard" in all future 123 agreements is ongoing in the U.S. government. [15]

With its many voluntary commitments, the UAE has set a positive nonproliferation example for other nuclear newcomer states. However, the UAE will need considerable foreign assistance and time to follow through on the nonproliferation pledges it has made. Without these, experts caution a "commitment-compliance gap" may emerge, whereby the UAE lacks the institutional capacity to fully adhere to its commitments. [16] This is of particular concern in the area of nonproliferation export controls, as the UAE only passed its first comprehensive nonproliferation export control legislation in 2007, and historically has been a major transit point for illicit transactions involving Iran and other neighboring countries. [17] The UAE has pledged its support for the Nuclear Suppliers Group's export control guidelines, and cooperated with efforts to bar shipments of sensitive technologies to Iran. [18] However, historically the UAE has reportedly housed "hundreds of front companies and foreign trading agencies that actively procure dual-use items for entities in countries under sanction." [19] Dubai's territory was a known hub for the A.Q. Khan network, which illicitly supplied nuclear technology to countries such as Iran, Libya, and North Korea. [20] While the UAE is making good-faith efforts to crack down on illicit trafficking, the development of robust export controls, border security, and related legal infrastructure requires significant time and resources.

The UAE faces capacity-building challenges in a number of areas beyond export controls. The nuclear program will require a significant long-term commitment to training domestic and regional personnel by the UAE and its foreign partners. In the meantime, the country will need to rely on foreign experts to ensure the safety and security of its nuclear program, a practice that some find problematic for the long-term sustainability of the program, while others note the additional transparency and access to the program foreign participation allow. The UAE appointed an International Advisory Board (IAB), headed by Hans Blix to provide independent assessment and an additional layer of transparency. The IAB issues semi-annual reports describing the UAE nuclear program's progress, and suggesting areas for improvement. [21] As in virtually all industry areas, the UAE relies heavily on foreign expertise, including in the highest management positions of the Emirates Nuclear Energy Corporation (ENEC) and its U.S.-modeled regulatory agency, the Federal Authority for Nuclear Regulation (FANR). The FANR is headed by a U.S. expert formerly employed by the U.S. Nuclear Regulatory Commission. [22]

IAEA assessments of the UAE's progress to-date have been favorable, with a December 2011 Integrated Regulatory Review Service team reporting that it was "impressed by the speed with which the UAE developed its regulatory framework and established a new regulatory body." [23] In June 2013, the UAE and the IAEA signed an Integrated Work Plan to facilitate interaction between the IAEA and the UAE's emerging nuclear power sector. [24]

Biological

The United Arab Emirates is a state party to the Biological and Toxin Weapons Convention (BTWC), and is not known to possess either biological weapons or programs for their development. [25]

However, the UAE is taking a regional leadership role in biotechnology issues, and will therefore need to develop robust export controls, biosecurity, and biosafety standards in order to mitigate the dual-use risks inherent to a large-scale biotechnology sector. In 2005, His Highness Sheikh Mohammed Bin Rashid Al Maktoum, Prime Minister of the UAE and leader of Dubai, announced that Dubai would build the world's first free-trade zone dedicated to biotechnology, with the intention of becoming the Middle East's regional biotechnology hub and a venue for international collaboration. [26] Completing construction in 2010, the Dubai Biotechnology & Research Park (DuBiotech) includes R&D, manufacturing, and conference space accommodating up to 160 laboratories. [27] With its promise of tax-free operation for at least fifty years and customs duty exemption on all goods and services, dozens of companies, including Pfizer, Amgen, Genzyme, and Merck, have begun operating at DuBiotech. [28] DuBiotech also offers conference venues, and has hosted biotechnology conferences on a range of issues including biosafety. [29] DuBiotech laboratories were built to biosafety level-3 standards. [30] Although the United Arab Emirates aspires to become a global biotechnology hub, the UAE is not a member of the Australia Group (AC). [31]

Chemical

The United Arab Emirates is a state party to the Chemical Weapons Convention (CWC) [32] The UAE is not known to possess either chemical weapons or programs for their development. [33]

The UAE will face increasing dual-use challenges requiring the development of robust export controls, chemical safety, and chemical security standards, as it is actively expanding its chemical industrial sector. In 2008, a Memorandum of Understanding (MOU) between the Abu Dhabi Investment Council and two chemical firms announced plans to develop a new Chemicals Industrial City in Abu Dhabi. [34] As envisioned, the Chemicals Industrial City would become the largest and most integrated chemical industry complex in the world, and a hub for petrochemical and other chemical products. [35] The project's timeline sets 2015 as the planned completion date. [36]

Missile

The United Arab Emirates is not a party to the Hague Code of Conduct Against Ballistic Missile Proliferation or the Missile Technology Control Regime (MTCR), but asserts it abides by MTCR guidelines. [37] However, in 1998 the UAE purchased an undisclosed number of Black Shaheen cruise missiles, which exceed MTCR capability limitations, from France and the United Kingdom. [38] The deal drew protests from the United States, who eventually conceded that "MTCR members have not always agreed with each others' interpretation of the MTCR guidelines." [39]

Despite its objections to the Black Shaheen deal, the United States has a significant strategic relationship with the UAE and has supplied it with numerous defensive systems. [40] In 2008, the UAE purchased the Patriot Guidance Enhanced Missile-T (GEM-T) and the Lockheed Martin Patriot Advanced Capability-3 (PAC-3) system from the United States. [41] Additionally, on 25 December 2011, the United States and the UAE signed an arms deal worth $3.48 billion dollars that included two Terminal High Altitude Area Defense (THAAD) systems, 96 missiles, two radar systems, spare parts, and training, making the UAE the first international recipient of the THAAD system, which is reportedly capable of "destroying incoming missiles at a range of 200 km." [42] In November 2012, the United States cleared the way for a sale of 48 THAAD missiles and associated equipment at an estimated cost of over $1 billion. [43] The UAE also purchased an unspecified number of the new AGM-88E Advanced Anti-Radiation Guided Missile

(AARGM) from the United States in April 2013. [44]

The UAE possesses an undisclosed number of SS-1 "Scud-B" (R-17) ballistic missiles, purchased from North Korea in 1989, with a range of 300km and a payload capability of 985kg. However, the missiles are reportedly non-operational. [45]

Sources

[1] "Non-Proliferation," Permanent Mission of the United Arab Emirates to the United Nations, www.un.int.
[2] "UAE adopts nuclear law," *World Nuclear News*, 5 October 2009, retrieved from www.world-nuclear-news.org.
[3] "International Nuclear Fuel Bank," NTI Projects: Nuclear Threat Initiative, www.nti.org; Ambassador Hamad Al Kaabi, "Intervention by UAE: Cluster 3 – General Issues," 2012 NPT Preparatory Committee, 9 May 2012.
[4] Bryan R. Early, "Strategies for Acquiring Foreign Nuclear Assistance in the Middle East: Lessons from the United Arab Emirates," Belfer Center for Science and International Affairs at the Harvard Kennedy School, June 2009, p. 5, http://belfercenter.ksg.harvard.edu.
[5] Ellen Tauscher, Under Secretary for Arms Control and International Security, "Agreement for Cooperation Between the Government of the United States of America and the Government of the United Arab Emirates Concerning Peaceful Uses of Nuclear Energy," statement before the House Foreign Affairs Committee, 8 July 2009.
[6] "Policy of the United Arab Emirates on the Evaluation and Potential Development of Peaceful Nuclear Energy," The Government of the United Arab Emirates, 20 April 2008, www.fanr.gov.ae.
[7] Christopher M. Blanchard and Paul K. Kerr, "The United Arab Emirates Nuclear Program and Proposed U.S. Nuclear Cooperation," Congressional Research Service, 10 March 2010, www.fas.org.
[8] "Policy of the United Arab Emirates on the Evaluation and Potential Development of Peaceful Nuclear Energy," The Government of the United Arab Emirates, 20 April 2008, www.fanr.gov.ae.
[9] "Policy of the United Arab Emirates on the Evaluation and Potential Development of Peaceful Nuclear Energy," The Government of the United Arab Emirates, 20 April 2008, www.fanr.gov.ae.
[10] Mark Holt, "U.S. and South Korean Cooperation in the World Nuclear Energy Market: Major Policy Considerations," Congressional Research Service, 21 January 2010, www.fas.org; "Nuclear Power in the United Arab Emirates," World Nuclear Association, March 2011, www.world-nuclear.org; Andrew England, "S. Koreans win $20bn UAE nuclear power contract," *The Financial Times*, 28 December 2008, www.ft.com; "Emerging Nuclear Energy Countries," World Nuclear Association, February 2012, www.world-nuclear.org; "Powering the future of the UAE through safe, clean and efficient nuclear energy," The Emirates Nuclear Energy Cooperation, www.enec.gov.ae; and Ayesha Daya and Stefania Bianchi, "U.A.E.'s Nuclear Power Program Said to Cost $30 Billion," *Bloomberg Businessweek*, 29 November 2011, www.businessweek.com.
[11] "UAE Nuclear Regulator Approves Barakah Power Plant Construction," Federal Authority for Nuclear Regulation, 18 July 2012, www.fanr.gov.ae; "United Arab Emirates and IAEA sign an Integrated Work Plan (IWP) to support the implementation of the national nuclear power programme," International Atomic Energy Agency, 6 June 2013, iaea.org.
[12] Kim So-hyun, "UAE to place order for four more nuclear power plants," *The Korea Herald*, 3 March 2012, www.koreaherald.com.
[13] Ambassador Thomas Graham, "123 Agreement for Nuclear Energy in the UAE: An Unprecedented and Responsible Step," *The Huffington Post*, 21 February 2012, www.huffingtonpost.com
[14] Mark Hibbs, "Saudi Arabia's Nuclear Ambitions," Carnegie Endowment for International Peace, 20 July 2010, www.carnegieendowment.org
[15] Elaine Grossman, "Administration Letter Provides "Case by Case" Approach to Nuclear Trade Deals," *Global Security Newswire*, 23 January 2012, www.nti.gsn.org.
[16] For more on the possibility of a "commitment-compliance gap," see: Bryan R. Early, "Export Control Development in the United Arab Emirates: From Commitments to Compliance," Belfer Center for Science and International Affairs at the Harvard Kennedy School, 6 July 2009, p. 7, http://belfercenter.ksg.harvard.edu.
[17] Bryan R. Early, "Export Control Development in the United Arab Emirates: From Commitments to Compliance," Belfer Center for Science and International Affairs at the Harvard Kennedy School, 6 July 2009, p. 7, http://belfercenter.ksg.harvard.edu.
[18] Bryan R. Early, "Export Control Development in the United Arab Emirates: From Commitments to Compliance," Belfer Center for Science and International Affairs at the Harvard Kennedy School , 6 July 2009, p. 7, http://belfercenter.ksg.harvard.edu; William Cohen and Sam Nunn, "Nuclear Cooperation with U.A.E. in our Interest," The Nuclear Threat Initiative, 3 June 2009, www.nti.org.
[19] William Cohen and Sam Nunn, "Nuclear Cooperation with U.A.E. in our Interest," The Nuclear Threat Initiative, 3 June 2009, www.nti.org. David Albright, Paul Brannan and Andrea Scheel, "Iranian Entities' Illicit Military Procurement Networks," The Institute for Science and International Security (ISIS), 12 January 2009, www.isis-online.org; William Cohen and Sam Nunn, "Nuclear Cooperation with U.A.E. in our Interest," The Nuclear Threat Initiative, 3 June 2009, www.nti.org.;

Elaine Shannon, "A New Nuke Black Market for Iran?" *Time*, 9 May 2007, www.time.com.
[20] Richard P. Conin, K. Alan Kronstadt, and Sharon Squassoni, "Pakistan's Nuclear Proliferation Activities and the Recommendations of 9/11 Commission: U.S. Policy Constraints and Options," Congressional Research Service, 24 May 2005, www.fas.org.
[21] "About Us," The International Advisory Board, 27 April 2012, www.uaeiab.ae.
[22] Chris Stanton, "New Law Sets UAE's Nuclear Age in Motion," 5 October 2009, www.thenational.aen.
[23] "IAEA Concludes Peer Review of UAE's Regulatory Framework," IAEA Press Release, 14 December 2011, www.iaea.org.
[24] "United Arab Emirates and IAEA sign an Integrated Work Plan (IWP) to support the implementation of the national nuclear power programme," International Atomic Energy Agency, 6 June 2013, iaea.org.
[25] William Faria, "Dubai's Biotechnology Park caters to Middle East," 28 January 2012, www.gulftoday.ae; "Weapons of Mass Destruction in the Middle East," Congressional Research Service, 14 January 2000.
[26] "The Premier Life Sciences Cluster in the Middle East," Dubai Biotechnology & Research Park, Dubai, UAE, www.dubiotech.ae, accessed 16 March 2012.
[27] "The Premier Life Sciences Cluster in the Middle East," Dubai Biotechnology & Research Park, Dubai, UAE, www.dubiotech.ae, accessed 16 March 2012; "DuBiotech succeeded in attracting and retaining 86 companies," *The Arab Hospital Magazine*, 25 October 2011.
[28] "DuBiotech: Dubai Biotechnology and Research Center," Dubai Biotechnology & Research Park, Dubai, UA, www.dubiotech.ae, accessed 16 March 2012; Press Release, "Ministry of Health and Dubai Customs to Raise Awareness against Counterfeit Medicines at Pharmaceutical Logistics Middle East 2012," Dubai Biotechnology & Research Park, 7 March 2012.
[29] "The Premier Life Sciences Cluster in the Middle East," Dubai Biotechnology & Research Park, Dubai, UAE, available at www.dubiotech.ae.
[30] "The Premier Life Sciences Cluster in the Middle East," Dubai Biotechnology & Research Park, Dubai, UAE, available at www.dubiotech.ae.
[31] The Australia Group, "Australia Group Participants," www.australiagroup.net.
[32] "Status of Participation in the CWC," Organisation for the Prohibition of Chemical Weapons, 21 May 2009, opcw.org.
[33] "Weapons of Mass Destruction in the Middle East," Congressional Research Service, 14 January 2000.
[34] Borealis News & Events, "New Chemical Industrial City planned for Abu Dhabi," Borealis AG, 19 March 2008.
[35] Borealis News & Events, "New Chemical Industrial City planned for Abu Dhabi," Borealis AG, 19 March 2008.
[36] "UAE economy projected to grow 3.9% in 2013," MENA Financial Network, 6 January 2013, menafn.com; Abu Dhabi Ports Company, "ADIC to develop Chemicals Industrial City in Tewaleh area," 5 May 2008.
[37] Karim Sadjadpour, "The Battle of Dubai: The United Arab Emirates and the U.S.-Iran Cold War," The Carnegie Endowment for International Peace, July 2011, p. 15, Carnegie website, www.carnegieendowment.org.
[38] "The UAE: Non-Proliferation," The Government of the United Arab Emirates, 20 April 2009, www.uae-embassy.org.
[39] Dennis M. Gormley, "Dealing with the Threat of Cruise Missiles," *Adelphi Paper 339* (2001): 40; "Ballistic and Cruise Missile Threat," National Air and Space Intelligence Center Wright-Patterson Air Force Base, April 2009, www.fas.org; Jeffery Lewis, "Storm Shadow, Saudi and the MTCR," Arms Control Wonk, 31 May 2011, www.armscontrolnetwork.com.
[40] Karim Sadjadpour, "The Battle of Dubai: The United Arab Emirates and the U.S.-Iran Cold War," The Carnegie Endowment for International Peace, July 2011, p. 15, www.carnegieendowment.org.
[41] "Raytheon Awarded $3.3 Billion Patriot Order for United Arab Emirates," *Inside Defense*, 31 December 2008.
[42] "Strategic Weapon Systems," *Jane's Sentinel Security Assessment – The Gulf States*, 13 June 2011. Other information on the deal available from: "U.S., UAE reach deal for missile-defense system," *CNN*, 30 December 2011, www.cnn.com; and Dan De Luce, "U.S. Arms Deal Bolsters UAE's Missile Defense," *Google News*, 31 December 2011, google.com.
[43] Defense Security Cooperation Agency, "News Release: United Arab Emirates – Terminal High Altitude Area Defense System Missiles (THAAD)," Transmittal No. 12-40, 5 November 2012, www.dsca.mil.
[44] Gopal Ratnam, "U.S. to Announce $10 Billion Arms to Israel, Saudis, U.A.E.," *Bloomberg*, 19 April 2013; "In changing region, US committed to military ties with Gulf Arabs," *Today's Zaman*, 2 May 2013.
[45] "Strategic Weapon Systems," *Jane's Sentinel Security Assessment – The Gulf States*, 13 June 2011; Joseph Bermudez, Jr., "A History of Ballistic Missile Development in the DPRK," p. 12. Monterey, CA: The Center for Nonproliferation Studies, 1999, cns.miis.edu.

NTI Nuclear Materials Security Index – 2014
Source: http://ntiindex.org/wp-content/uploads/2014/01/2014-NTI-Index-Report1.pdf

UAE – Hamad Alkaabi joins Nuclear Threat Initiative board

Source: http://www.thenational.ae/uae/technology/hamad-alkaabi-joins-nuclear-threat-initiative-board

Feb 05 – Hamad Alkaabi, the UAE's permanent representative to the International Atomic Energy Agency (photo), is one of three new additions to the Nuclear Threat Initiative (NTI) board of directors.

The NTI is a non-profit, non-partisan organisation that seeks to reduce threats from nuclear, biological and chemical weapons. Mr Alkaabi, who is also the UAE's special representative for international nuclear cooperation, joins Gideon Frank and Paul Otellini as the newest members of the NTI board.

Mr Frank is a former director general of the Israel Atomic Energy Commission, while Mr Otellini is a former president and chief executive of Intel Corporation.

Mr Alkaabi helped to lead the initial assessment of nuclear power in the UAE, and has since served as the country's primary interlocutor on international issues regarding nuclear energy and non-proliferation.

"Ambassador Alkaabi helps guide his country's nuclear energy programme, the model for any country seeking a peaceful approach that doesn't contribute to proliferation. NTI will benefit from his expertise, as we consider how to tap the opportunities of nuclear energy while minimising risks," said Ted Turner, an NTI co-chairman.

NTI president Joan Rohlfing said the three men would "bring a unique and fresh perspective to NTI, which is critical as we develop new strategies to build a safer world".

UAE – ENEC completes concrete dome for Unit 1 reactorcontainment builing

Source: http://www.enec.gov.ae/media-centre/news/content/enec-completes-concrete-dome-for-unit-1-reactor-containment-building

Jan 13 – UAE peaceful nuclear energy program is progressing on schedule. **The Emirates Nuclear Energy Corporation (ENEC) today announced the completion of the construction of the concrete dome for the Unit 1 Reactor Containment Building.**

KOREA ELECTRIC POWER CORPORATION
مؤسسة الإمارات للطاقة النووية
Emirates Nuclear Energy Corporation
SAMSUNG
Unit 1 RCB Dome Completion Ceremony, Barakah, December 2014
HYUNDAI

The completion of the dome earlier this week marks the achievement of another on-time milestone in the complex construction of the UAE's first nuclear energy plant. The dome is the final structural component of the vast Reactor Containment Building (RCB), which now measures more than 70 metres in height.

The RCB houses the nuclear reactor and is a critical structure in the nuclear plant's defence-in-depth barriers. RCBs are extremely robust in design; with thick concrete walls and heavy reinforcing steel, they rank among the strongest structures in the world. They are designed to confine and contain radiation, even in the most extreme circumstances.

"We are proud to maintain our track record of achieving key construction milestones safely and on time," said Mohamed Al Hammadi, Chief Executive Officer of ENEC. "The RCB is a critical structure in the plant's safety and security. The construction of this structure has involved thousands of people who have all shown their commitment to the highest standards of quality and safety at all times."

Qatar
Arabian Gulf
Abu Dhabi
Braka
Saudi Arabia
United Arab Emirates
Oman

"We remain confident and committed to successfully delivering our mission of safe, clean, reliable and efficient nuclear energy to the UAE in 2017," added Mr Al Hammadi.

Construction of the RCB commenced in July, 2012 with the fabrication of the basemat. The Containment Liner Plate, which forms the inner floor, wall and ceiling of the RCB, was then fabricated and installed in 19 stages over a period of 10 months. **The dome, which measures 51.4 metres in diameter, 24 meters in height and weighs approximately 9000 metric tonnes**, has been constructed over the past five months in nine stages. The next phase of work on the RCB will involve the installation of the containment post tensioning system, which is used for pre-stressing the concrete structure, followed by a three-month structural integrity test.

Overall, Unit 1 is now more than 60 per cent complete and on track to commence commercial operations in 2017, pending further regulatory approvals. The indicative timeline for the other nuclear energy plants is for Unit 2 to begin operations in 2018, Unit 3 in 2019 and the final Unit 4 in 2020.

Following a rigorous 18-month review by the UAE Federal Authority for Nuclear Regulation (FANR) and a team of international nuclear energy experts, the regulator granted ENEC approval to commence construction of units 3 and 4 this earlier year. Pouring of the first safety concrete for Unit 3 was announced in September 2014.

When the four reactors are completed in 2020, the UAE's nuclear program will provide approximately 25% of the UAE's electricity needs, saving up to 12 million tons of greenhouse gas emissions each year.

Hundreds of Contaminated High-Risk Former Nuclear Facilities Still Awaiting Cleanup

By Amanda Vicinanzo (Senior Editor)

Source: http://www.hstoday.us/single-article/hundreds-of-contaminated-high-risk-former-nuclear-facilities-still-awaiting-cleanup/f73cc59a7765a9024e4f1f192bb4d0f9.html

Hundreds of contaminated facilities left in the wake of 50 years of nuclear weapons production and energy research during the Cold War and Manhattan Project are still years away from being cleaned up, according to a recent audit report by the Department of Energy's (DOE) Inspector General (IG).

"Almost 50 percent of these facilities are more than 50 years old and are becoming dangerous," the IG said. "Several of the facilities are in such disrepair that maintenance and nonessential utilities are limited or discontinued, and access by workers has been prohibited. The longer these facilities remain unaddressed, the further they degrade, and the more dangerous and costly they are to maintain or disposition."

DOE created the Office of Environmental Management (OEM) in 1989 to oversee cleanup of the contaminated facilities. However, due to increasing workloads and budgetary constraints, in 2001 it stopped accepting additional facilities from other mission programs. In 2007, it began accepting facilities from other programs if certain criteria for transfer were met.

In February 2009, OEM identified **292** excess contaminated facilities that met its transfer criteria and that it would accept once funding became availability. **58 facilities were demolished and decommissioned, but 234 remained.**

DOE has yet to create a transfer schedule for the 234 facilities, some of which are known to be contaminated by dangerous elements. Although the contaminated facilities pose significant health and safety risks, DOE continues to lag behind in addressing the backlog of excess contaminated facilities and materials requiring clean up.

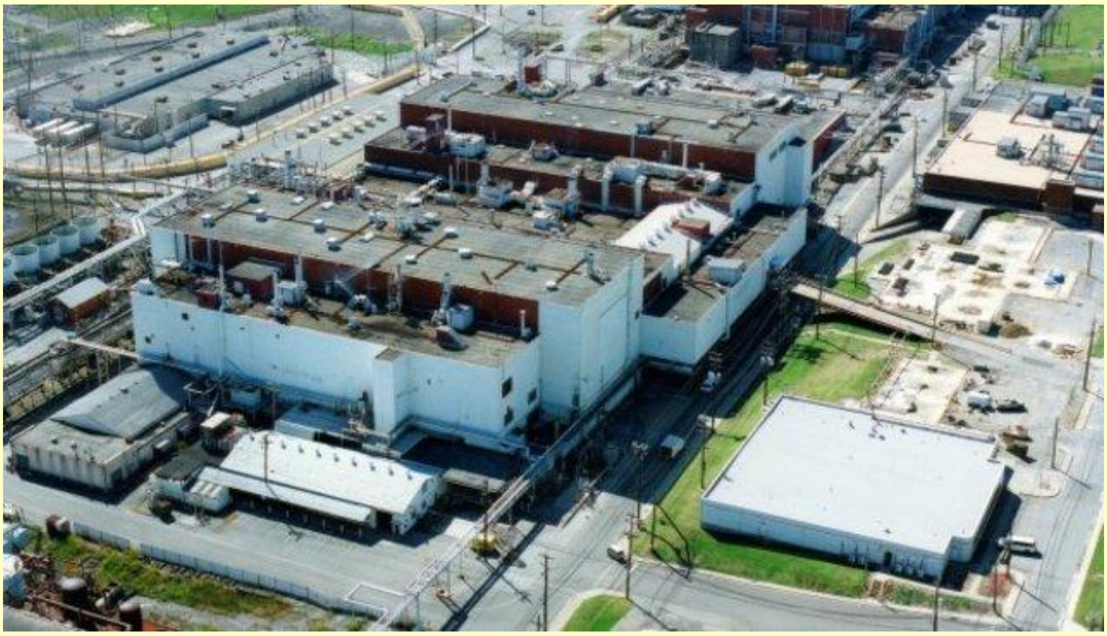
Moreover, OEM officials have indicated the transfer date will actually be extended to as late as 2035 despite the fact that many of these facilities are contaminated with dangerous elements—including uranium, mercury, and beryllium—which pose a health and safety risk. These chemicals have been known to leach to soil and groundwater during weather-related events.

In a prior report, the IG commented that, “The degradation within these facilities ranged from failures in critical structural components to high levels of contamination.” The facilities pose a high level of risk to department employees as well as communities surrounding the facilities.

DOE officials cite budget constraints as the chief reason behind the slow cleanup up of the high-risk contaminated facilities. However, the IG found DOE has yet to develop a strategy for using its limited cleanup funds to reduce the risk posed by the contaminated facilities.

“Delays in the cleanup and disposition of contaminated excess facilities expose the Department, its employees and the public to ever-increasing levels of risk,” the IG’s report said. “While surveillance and maintenance is intended to control these risks, delays in decommissioning and demolition also lead to escalating disposition costs.”

The IG added, “Further, deferral of tackling these liabilities in a timely manner may affect ongoing mission work, as well as plans to expand and accommodate new missions that are needed to meet energy and national security objectives.”



One of the facilities, the Alpha-5 building at Y-12 (photo above), was described by the National Nuclear Security Administration (NNSA) as the "worst of the worst.” Built in 1944, the facility has supported a number of missions that used materials such as uranium, mercury and beryllium. It ceased operation in 2005 and has experienced severe degradation since then.

According to the IG, "During a 2008 Environmental Management assessment, it was noted that the facility had substantial flooding, exterior piping and associated supports were corroding, and reinforced concrete roof panels had deteriorated. The assessment concluded that the combination of the large facility size, rapidly deteriorating conditions, and vast quantity of items requiring disposition made this facility one of the greatest liabilities in the Department's complex."

A 2014 NNSA assessment discovered that significant roof deterioration had allowed for water intrusion, which in turn allowed the spread of radiological and toxicological contamination. The contaminants in the facility also put the facility at risk for explosion. NNSA concluded that the facility posed a significant risk to workers and the environment. The condition of the facility "should not be accepted," NNSA said.

"Due to delays in the cleanup and disposition of contaminated excess facilities, the department is taking on ever-increasing levels of risk," the IG said.

The IG concluded that the department needs to focus its resources on its highest risk priorities. To do this, the department must develop a corporate approach to identifying and scheduling facilities for transfer to OEM.

Specifically, the IG recommended the Offices of the Under Secretary for Nuclear Security, Under Secretary for Science and Energy and Under Secretary for Management and Performance develop an analysis and report on the Department's contaminated excess facilities and evaluate alternatives for the disposition of excess facilities based on this analysis.

The department concurred with the IG's recommendations.

If Iran Develops Nuclear Weapons, Syria Could Come Under its Nuclear Umbrella

By Debalina Ghoshal

Source: http://www.diplomaticourier.com/news/regions/middle-east/2465-if-iran-develops-nuclear-weapons-syria-could-come-under-its-nuclear-umbrella

Although Iran has claimed that the aims of its nuclear program are peaceful, these statements have not been viewed as credible in the West. These fears worsened in 2012 after reports from the International Atomic Energy Agency (IAEA) confirmed Iran was producing uranium enriched at a 20 percent level. As talks regarding Iranian uranium enrichment continues, the dilemma that arises is how much of uranium enrichment should be allowed by the United States.

Even more concerning to the United States and its Western allies is the likelihood that Syria could come under Iran's nuclear umbrella, whether by hosting command and control facilities or through Iran's development of delivery systems which could be nuclear capable (particularly missiles) that provide extended nuclear deterrence. **Syria desires access to weapons of mass destruction because it views its neighbors Turkey and Israel as staunch adversaries.** According to Antony Cordesman of Centre for Strategic and International Studies, nuclear weapons would provide Syria some kind of "parity" with Israel and "some status within the region." Turkey is under the NATO nuclear umbrella, and though Israel's official nuclear status continues to be ambiguous, it is widely believed to possess numerous nuclear weapons.

Syria first obtained chemical weapons in the early 1980s to counter the perceived Israeli threat, but these weapons have more recently been used by Damascus to fight the ongoing civil war against its own people. And despite being party to the Nuclear Non-Proliferation Treaty and supporting a Nuclear Weapon-Free Zone in the Middle East, **Syria still has ambitions to acquire nuclear weapons**. In 2011, UN investigators identified an unknown complex in Syria which led them to believe that Syria worked closely with A.Q. Khan of Pakistan to develop nuclear weapons. However, reports suggest that such plans of developing nuclear weapons could have been abandoned by Syria after Israel destroyed their plutonium production reactor.

Moreover, according to NTI Reports, Syria's weak industrial infrastructure, poor scientific capabilities, and lack of trained engineers needed to run a "weapons-oriented program" require it to depend on external assistance. While Syria could look towards various states for assistance (like Pakistan, China, or Russia) in building a nuclear program to compete with its neighbors, living under the Iranian nuclear umbrella would be more technologically and economically feasible. It would also allow them a way around violating the Nuclear Non-Proliferation Treaty.

Meanwhile, Iran has been interested in providing a security umbrella to other Muslim states in the Middle East, and it already has a long-standing commitment to sustain its influence over Damascus. **Because Iran has always backed Syrian President Bashar Assad, Syria could be incorporated under Tehran's nuclear umbrella.** Syria is also advantageous for Iran since it makes it easy to transfer arms to anti-Israel forces like Hezbollah in Lebanon.

News reports have indicated Syria is developing improved versions of **Khaybar1 missiles** (photo left) under Iranian supervision and is also replacing liquid-fuel missiles with solid-fuel missiles for use by Hezbollah. And according to Stimson Center President Ellen Laipson, Syria is already the link that connects Tehran to Hezbollah, serving as a "critical forward base and springboard to eventual regional domination" for Iran. This is because Syria's leaders have always "projected a self-image of enduring greatness and leadership of the pan-Arab cause."

According to Yaakov Peri, a former head of Shin Bet and current Israeli Minister of Science and Technology, Iran's incorporation of Syria under its nuclear umbrella could make Syria a "launch pad for terrorist ideology and activity" that would threaten Israel and the broader region. Israel is particularly concerned about nuclear weapons falling into the hands of Hezbollah after reports suggested that Assad is "facilitating the transit of advanced Iranian arms" to the group.

Would Iran defy a deal from the P5+1 negotiations? Even though President Rouhani aspires to improve the economy of Iran and also improve Tehran's relations with the international community, other Iranian leaders have different views about Iran's nuclear program. Although Iran has positively engaged in the nuclear negotiations, there are still tensions, including a new Republican-led Congress in the U.S. threatening harsher sanctions (and occasionally using rhetoric about bombing Iranian nuclear facilities).

Iran's efforts to strengthen its regional hegemony in the region could result in Tehran providing extended nuclear deterrence to its neighbors in the Middle East. However, at this point, the United States should feel the urgency of ensuring that Tehran does not develop nuclear weapons since such weapons could fall into the hands of terrorist organizations, such as ISIS, in Syria**. If Iran extends a nuclear umbrella to Syria, it will only increase the pace of the arms race in the Middle East.**

***Debalina Ghoshal** is an Associate Fellow for the Centre for Air Power Studies in New Delhi.*

Nuclear powerScientists develop accident-tolerant nuclear fuels

Source: http://www.homelandsecuritynewswire.com/dr20150211-scientists-develop-accidenttolerant-nuclear-fuels

Feb 11 – The summer of 2014 marked an important milestone toward further innovation in the nation's nuclear plants regarding the development of light water reactor nuclear fuel with enhanced accident tolerant characteristics.

For several years, nuclear researchers have designed, fabricated and tested a host of novel nuclear fuels and fuel cladding materials (enclosed tubes that house the fuel in a reactor) in laboratories across the U.S. Now, testing of promising fuels and materials with enhanced accident tolerant characteristics in a U.S. nuclear test reactor is commencing. Scientists and engineers from research labs and industry have prepared advanced concepts for insertion into Idaho National Laboratory's Advanced Test Reactor.

An INL release reports that these efforts are central to the Department of Energy's Advanced Fuels Campaign. Prior to the unfortunate events at the Fukushima-Daiichi nuclear power plants in Japan, the Fuels Campaign focused on development of higher performance fuels that could offer opportunity for power uprates or allow use of the fuel in a reactor for longer periods of time. Following the accident in Japan, this research shifted to include both higher performance and enhanced tolerance to severe, beyond design basis accident conditions.

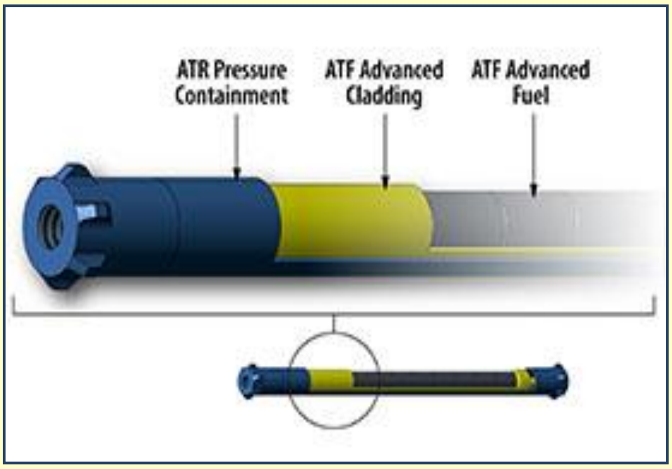
The proposed light water reactor (LWR) fuel and cladding improvements center on an increased tolerance to postulated beyond design basis accident scenarios within a nuclear reactor. Several adjustments target fuel and cladding physical integrity under severe accident conditions, including enhanced retention of fission products and resistance to increased temperature. Certain novel compositions look at chemical properties as well.

The advanced LWR fuels and claddings that will be tested contain a range of modifications to the current LWR fuel system to improve fuel performance in addition to enhancing safety characteristics. Desirable performance attributes include increased power density, longer fuel cycle and operation to higher burnup. In other words, in addition to characteristics of enhanced accident tolerance, these new fuels have the

potential to last longer and produce more energy.

For example, one technology of interest is silicon carbide-based cladding. Shannon Bragg-Sitton, the Deputy National Technical Director for the Advanced Fuels Campaign, explained the possible advantages this cladding could offer.

“In Fukushima, the fuel’s zirconium cladding reacted with high temperature steam to produce hydrogen. This ultimately resulted in the explosions that were observed when the hydrogen was combusted,” Bragg-Sitton said. “A silicon carbide cladding would still react with high temperature steam, but the reactions would occur at a much slower rate with massively reduced hydrogen production. Responders would have more time to mitigate the problem.”



This cutaway illustration shows the ATF-1 irradiation capsule assembly containing the fuel and cladding for the test rodlet.

Final assembly of ATR experiments occurs at the nearby Test Train Assembly Facility.

The technologies that have been prepared for insertion into the Advanced Test Reactor have been developed by three different industry teams — Westinghouse, AREVA, and General Electric. These small-scale rodlet experiments include both novel fuel variants in standard cladding and novel cladding on standard fuel.

Test rodlet capsules have been fully assembled and will begin irradiation in early 2015. **These experiments are referred to as the “ATF-1” test series.** Additional fuel and cladding concepts may be inserted into the reactor for testing later in 2015.

The ATF-1 experiments mark the beginning of four new test series for the Advanced Fuels Campaign. The first series will evaluate interactions between the fuel and its cladding. The materials will be irradiated in the test reactor for different lengths of time and examined for performance. The most promising concepts will advance to the next round of tests.

The remaining three LWR accident tolerant fuel test series will also be conducted at INL. The second series will be conducted in the Advanced Test Reactor and will measure fuel-cladding and cladding-coolant interactions using a water test loop. The third and fourth test series will be conducted at INL’s Transient Reactor Test (TREAT) facility.

Similar to automobile safety testing, the TREAT reactor can be used to push fuel and cladding inserted in an experiment location to failure to determine the maximum conditions the materials can withstand. Between the third and fourth series, a lead fuel rod, containing the most promising fuel or cladding material concepts, is planned for demonstration in a commercial nuclear reactor. After each phase of testing and evaluation, the list of concepts will be further down-selected, or prioritized, until only the most promising options are left.

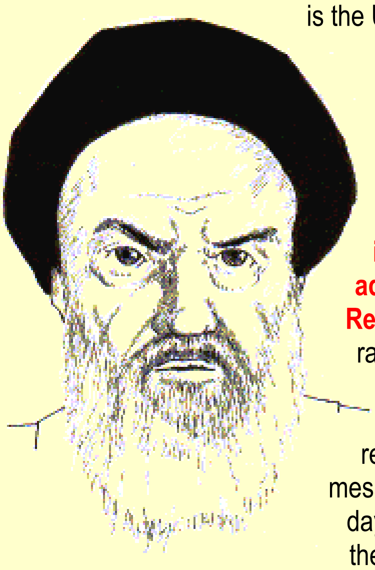
“I think we have some good concepts to work with,” Bragg-Sitton said. “The projects we’re developing now could significantly impact nuclear energy in both the short and long term. Putting these concepts with enhanced accident tolerant characteristics into the Advanced Test Reactor now is a big step toward the further innovation of the U.S.'s current nuclear system."

The Only Thing Scarier Than Iran's Nukes

By James S. Robbins

Source: http://nationalinterest.org/feature/the-only-thing-scarier-irans-nukes-12231

Feb 12 – Denying Iran nuclear-weapons capability is not only a means of limiting the proliferation of weapons of mass destruction. It is also part of a broader ideological struggle that Tehran is taking much more seriously than is the United States.



This month, Iran celebrates the 36th anniversary of the return of the Ayatollah Ruhollah Khomeini from exile in 1979 and the advent of the Islamic Revolution. In speeches, rallies and state-sponsored television shows, Tehran is reaffirming the messages of the heady days of the downfall of the Shah, the supremacy of Shi'a Islam and the destruction of Iran's enemies, particularly Israel and the United States. The celebration reminds us that Iran is not just a Middle Eastern adversary state with dreams of regional hegemony. It is a revolutionary regime seeking to reshape the map of the region, and the belief system of the world.

Tehran remains committed to its revolutionary agenda. Today, Iran is active in promoting its ideology in Iraq and Afghanistan. Iran supports the largest international terrorist network in the world, including backing Hezbollah and Hamas. Iranian-backed Houthi rebels in Yemen have captured vast swathes of territory and disrupted the established government. This is a revolution in action, and it illustrates that Tehran is not simply seeking to extend its influence in the region. Rather, it is working to impose Khomeini's Shi'ite Islamist agenda beyond its borders.

Yet the White House is loathe to wage a war of ideas with Iran. Given President Obama's well-documented sensitivities regarding Islam, his administration prefers to focus on other aspects of the effort to achieve global stability. Jihadist terror groups such as the Sunni-aligned ISIS or pro-Tehran Houthis are termed "violent extremists." The Western rivalry with Iran is reduced to the language of power politics, ignoring the ideological dimension.

But Iran is not seeking nuclear-weapons capability simply to preserve its regime; it is also doing so to extend its revolution. When Iran can deter the use of force, it can also increase the reach of its ideas. And if Washington refuses to promote a convincing counterargument for freedom, it is unilaterally disarming.

Tehran, meanwhile, is not timid about promoting its vision in the West. In January, in the wake of the jihadist attack on the offices of the magazine *Charlie Hebdo* in Paris, Iranian Supreme Leader Ayatollah Ali Khamenei penned an open letter to the youth of the West making the case for Islam. He maintained that the view of Islam most young people receive is filtered through hostile governments and negative press reports. He asked why "attempts are made to prevent public awareness regarding an important issue such as the treatment of Islamic culture and thought" and encouraged young people to "study and research the incentives behind this widespread tarnishing of the image of Islam." As well, Khamenei asked them to study the Koran themselves, because, he said, "the future of your nations and countries will be in your hands." For its part, the White House is making little effort to promote the cause of freedom among Iran's youth, even though—given the radical, repressive nature of that regime—it is likely to be a much easier idea to sell.

Focusing only on the nuclear dimension of the Iranian threat is a mistake, because the ideological conflict is the root cause of the problem. Absent Tehran's revolutionary aspirations, there would be no drive to acquire weapons of mass destruction and no Iranian-backed global terrorist network. Arms-control agreements, verification regimes and contentious international inspections cannot guarantee that Iran is not still secretly developing nuclear weapons.

When a regime leads its people in chants of "death to America," we should do them the courtesy of believing that they mean it.

James S. Robbins *is Senior Fellow in National Security Affairs at the American Foreign Policy Council in Washington, DC.*

Nuclear weapons - reading the signs of the times

By Noel Stott

Source:http://www.defenceweb.co.za/index.php?option=com_content&view=article&id=38101:iss-nuclear-weapons-reading-the-signs-of-the-times&catid=113:international-news&Itemid=248

Feb 20 – Last month, the Bulletin of Atomic Scientists announced that it had moved its so-called Doomsday Clock three minutes closer to midnight. The Doomsday Clock is internationally recognised as an indicator of how close we are to destroying ourselves with advanced equipment and technologies, most importantly with nuclear weapons.

August this year marks the 70th anniversary of the destruction of Hiroshima and Nagasaki by United States (US) nuclear weapons.

In May, it will have been 20 years since the Treaty on the Non-Proliferation of Nuclear Weapons (NPT) was indefinitely extended to allow more time for states to implement their commitment to the 'cessation of the nuclear arms race at an early date' and 'to nuclear disarmament.'

Now more than ever, countries with nuclear weapons need to read the signs of the times by reflecting deeply on current events and responding to them appropriately. Nine states currently possess such weapons, namely the US, United Kingdom (UK), China, France, India, Israel, Pakistan, North Korea and Russia. In contrast, 115 states or some 60% of United Nations (UN) member states, including all African states, have committed to not producing, acquiring, testing or possessing nuclear weapons.

According to the Stockholm International Peace Research Institute (SIPRI), the nine states above own approximately 4 000 operational nuclear weapons and a combined total of about 16 300 nuclear weapons. While none have been used since 1945, Robert Gard – a retired army lieutenant general – says that in the US at least 1 200 'significant' accidents involving nuclear weapons occurred between 1950 and 1968. Furthermore, in 1980 a dropped wrench led to a fatal explosion of a nuclear missile in Arkansas, and in 1961, two nuclear devices were mistakenly dropped over North Carolina – but luckily did not detonate as they had not been 'armed'.

Last year, in a message to the December Vienna Conference on the Humanitarian Impact of Nuclear Weapons, Pope Francis questioned the ethical basis to the so-called doctrine of nuclear deterrence, stating that the 'ethical and humanitarian consequences of the possession and use of nuclear weapons are catastrophic and beyond the rational'. He added: 'If it is unthinkable to imagine a world where nuclear weapons are available to all, it is reasonable to imagine a world where nobody has them.

'Nuclear deterrence and the threat of mutually assured destruction cannot be the basis for an ethics of fraternity and peaceful coexistence among peoples and states.' He thus joined the majority of the world's states in calling for nuclear weapons to be banned 'once and for all' – even though for years, and especially during the Cold War, the Catholic Church accepted that the concept of nuclear deterrence was morally justifiable.

Pronouncements such as these have gravity in Africa. Since 1970, Catholicism has seen a global shift southwards, with a recent study showing that the continent's Catholic population is now at more than 175 million. It is little wonder that the UN-based Africa Group also called for the development of a legally binding instrument to prohibit nuclear weapons. The Pope, however, is not alone in calling for the elimination of nuclear weapons. At the same meeting, which followed similar events in Norway in March 2013 and Mexico in February 2014, some 158 governments, numerous international organisations and various civil society groupings outlined the catastrophic humanitarian consequences of the use of nuclear weapons.

These changes come at a time when the Republic of the Marshall Islands has sued all nine nuclear weapon states, accusing them of violating their duty to negotiate the elimination of nuclear weapons.

They further allege that this exposes Marshallese communities to the dangers of nuclear arsenals and the probability that other states will want to develop such destructive weapons.

Further, in a recent letter addressed to parishioners of the UK's Church of England, the House of Bishops called for a proper debate on Trident (Britain's nuclear submarine fleet), stating that 'shifts in the global strategic realities mean that the traditional arguments for nuclear deterrence need re-examining [and that] the presence of such destructive capacity pulls against any international sense of shared community'.

In addition, in October last year, 155 states, including all the members of the African Union, expressed that awareness of the catastrophic consequences of nuclear weapons ought to underpin all approaches and efforts towards nuclear disarmament. In a joint statement on the humanitarian consequences of nuclear weapons at the UN, they said 'all efforts must be exerted to eliminate the threat of these weapons of mass destruction,' adding that 'the only way to guarantee that nuclear weapons will never be used again is through their total elimination.'

Nuclear weapons states would do well to read the signs of the times reflected in recent developments ahead of the forthcoming 2015 NPT Review Conference. They need to be open and transparent about what steps they will take to achieve and maintain a nuclear-weapon-free world. They also need to urgently announce a time-bound commitment to prohibit and eliminate nuclear weapons in light of their unacceptable humanitarian consequences and associated risks.

Progressive governments, international organisations such as the International Committee of the Red Cross (ICRC) and global civil society, including in Africa, have vowed to 'identify and pursue effective measures to fill the legal gap for the prohibition and elimination of nuclear weapons.' Taking the lead from one of the outcomes of the Vienna Conference, they have pledged to 'follow the imperative of human security for all and to promote the protection of civilians against risks stemming from nuclear weapons'.

As Peter Maurer, President of the ICRC recently stated, 'reducing the risk of nuclear-weapon use and ensuring their elimination through a legally binding international agreement is a humanitarian imperative, and it is time for states, and all those of us in a position to influence them, to act with urgency and determination to bring the era of nuclear weapons to an end.' Now is the time for the nine nuclear weapon states to join this endeavour.

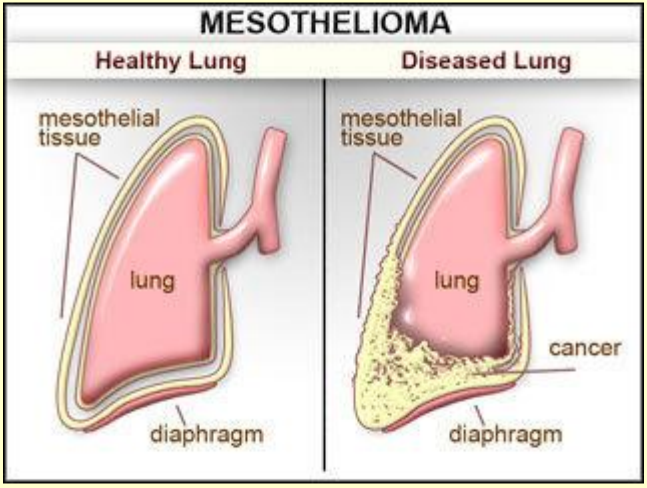
__Noel Stott__ is Senior Research Fellow, Transnational Threats and International Crime Division, ISS Pretoria.

Researchers Warn of Higher Mesothelioma Risk in Nuclear Plant Workers

Source: http://globalbiodefense.com/2015/02/10/researchers-warn-higher-mesothelioma-risk-nuclear-plant-workers/?sthash.OHCJTpFi.mjjo#sthash.OHCJTpFi.hVRe9tVh.dpuf

Feb 10 – Radiation-related cancers are not the only health threat to former nuclear plant workers, according to a new published report from the Center for Construction Research and Training and Duke University.

The report finds that **people who worked at a DOE nuclear site have a higher risk of death from "all causes, all cancers", including the asbestos-related cancer mesothelioma.**



"Mortality was elevated for all causes, all cancers, cancer of the trachea, bronchus, and lung and lymphatic and hematopoietic system, mesothelioma, COPS, and asbestosis," writes co-author Dr. Knut Ringen.

The report, published in the *American Journal of Industrial Medicine,* was based on data from more than 18,800 workers who were part of the Building Trades National Medical Screening Program.

"The central message of this study is that nuclear site workers are not 'out of the woods' in terms of their health. Mesothelioma and asbestosis can manifest even decades after exposure, which is why it is especially important for people who worked in these jobs to know and be able to recognize the symptoms," says Alex Strauss, Managing Editor of Surviving Mesothelioma.

Mortality of older construction and craft workers employed at department of energy (DOE) nuclear sites: Follow-up through 2011

By Knut Ringen Dr. PH[1], John Dement PhD[2], Laura Welch MD[1], Eula Bingham PhD[3], Patricia Quinn[1], Anna Chen[4] and Scott Haas[4]

[1]The Center for Construction Research and Training, Seattle, Washington
[2]Division of Occupational and Environmental Medicine, Duke University Medical Center, Durham, North Carolina
[3]Department of Environmental Health, University of Cincinnati Medical Center, Cincinnati, Ohio
[4]Zenith American Solutions, Covina, California

Background – The Building Trades National Medical Screening Program (BTMed) was established in 1996 to provide occupational medicine screening examinations for construction workers who have worked at US Department of Energy nuclear sites. Workers participating in BTMed between 1998 and 2011 were followed to determine their vital status and mortality experience through December 31, 2011.
Methods - The cohort includes 18,803 BTMed participants and 2,801 deaths. Cause-specific Standardized Mortality Ratios (SMRs) were calculated based on US death rates.
Results - Mortality was elevated for all causes, all cancers, cancers of the trachea, bronchus, and lung and lymphatic and hematopoietic system, mesothelioma, COPD, and asbestosis.
Conclusions - Construction workers employed at DOE sites have a significantly increased risk for occupational illnesses. Risks are associated with employment during all time periods covered including after 1980. The cancer risks closely match the cancers identified for DOE compensation from radiation exposures. Continued medical surveillance is important. Am. J. Ind. Med. 58:152–167, 2015.

Missing radioactive material may pose 'dirty bomb' threat: IAEA

Source: http://www.reuters.com/article/2014/03/21/us-nuclear-security-iaea-idUSBREA2K10W20140321

March 2014 – **About 140 cases of missing or unauthorized use of nuclear and radioactive material were reported to the U.N. atomic agency in 2013,** highlighting the challenges facing world leaders at a nuclear security summit next week.

Any loss or theft of highly enriched uranium, plutonium or different types of radioactive sources is potentially serious as al Qaeda-style militants could try to use them to make a crude nuclear device or a so-called "dirty bomb", experts say.

Denis Flory, deputy director general of the International Atomic Energy Agency (IAEA), said most of the reported incidents concerned small quantities of radioactive material.

But, "even if they can't be used for making a nuclear weapon, they can be used in radioactive dispersal devices, which is a

concern," Flory told Reuters in an interview.

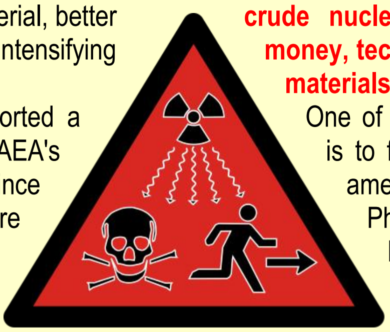
In a "dirty bomb", conventional explosives are used to disperse radiation from a radioactive source, which can be found in hospitals, factories or other places that may not be very well protected.

Holding a third nuclear security summit since 2010, leaders from 53 countries - including U.S. President Barack Obama - are expected to call for more international action to help prevent radical groups from obtaining atomic bombs.

At the March 24-25 meeting in The Hague, they will say that much headway has been made in reducing the risk of nuclear terrorism but also make clear that more must be done to ensure that dangerous substances don't fall into the wrong hands.

The Dutch hosts say the aim is a summit communique "containing clear agreements" to prevent nuclear terrorism by reducing stockpiles of hazardous nuclear material, better securing such stocks and intensifying international cooperation.

Flory said member states had reported a total of nearly 2,500 cases to the IAEA's Incident and Trafficking Database since it was set up two decades ago. More than 120 countries take part in this information exchange project, covering theft, sabotage, unauthorized access and illegal transfers.



Nuclear Security Pact delayed

In 2012, 160 incidents were reported to the IAEA, of which 17 involved possession and related criminal activities, 24 theft or loss and 119 other unauthorized activities, its website says.

"It is continuing, which means there is still a lot of work to do to have that really decrease," Flory said with respect to the statistics. However, there are also "more and more countries which declare incidents. The number of incidents we don't know is probably decreasing."

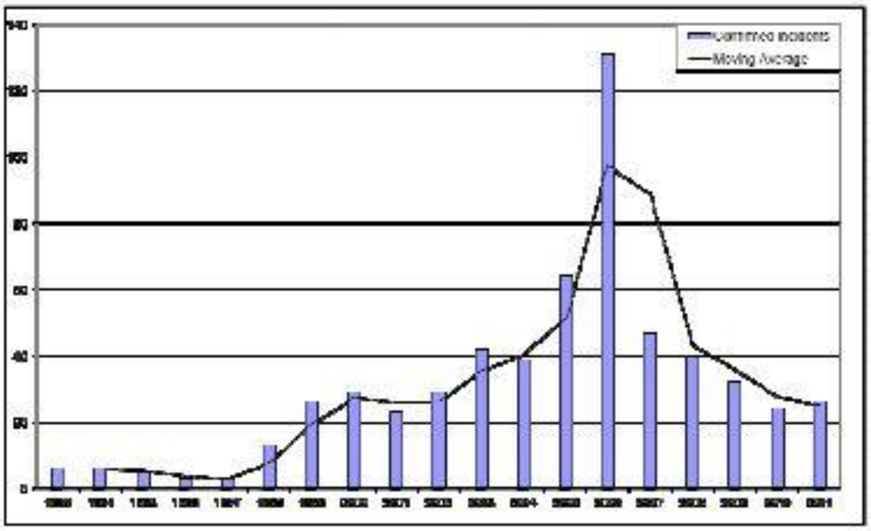
Because radioactive material is less hard to find and the device easier to make, experts say a "dirty bomb" - which could cause panic and have serious economic and environmental consequences - is a more likely threat than a deadly atom bomb.

Radical groups could theoretically build a crude nuclear bomb if they had the money, technical knowledge and fissile materials needed, analysts say.

One of the biggest challenges ahead is to finally bring into force a 2005 amendment to the Convention on Physical Protection of Nuclear Materials (CPPNM), Flory said.

There are still 27 countries - including the United States - which need to ratify the amendment, which expands the coverage from only the protection of nuclear material in international transport to also include domestic use, transport and

Confirmed incidents involving theft or loss, 1993–2011



storage.

"It is extremely important because this amendment brings a lot of strengthening in the field of nuclear security," he said.

Harvard University professor Matthew Bunn said this month that a U.S. failure so far to ratify the amended convention "has made it far harder" for Washington to pressure others to do so.

"The problem appears to be a combination of lack of sustained high-level attention by both the administration and Congress and disputes over unrelated issues," Bunn said.

Flory, who heads the IAEA's nuclear safety and security department, said he knew that the U.S. administration was "very keen on finishing the process" as soon as possible.

"This is a country where you have a lot of nuclear material, a lot of nuclear facilities and they have a lot of influence on nuclear security."

When you said this is the hot, new wine from Los Alamos, you weren't kidding.

Counter IED Report – Winter 2014/2015

Source: http://issuu.com/deltabusinessmedialimited/docs/counter-ied_report_winter_2014-15_e?e=6269486/11144445

Buster saved my life every day we were together'

Source: http://www.telegraph.co.uk/lifestyle/pets/11384818/Buster-saved-my-life-every-day-we-were-together.html

RAF Police Flight Sergeant Will Barrow & his dog Buster. Buster served 5 tours of duty in Bosnia Afghanistan and Iraq, with Will and is the subject of a new book Photo: Philip Hollis/The Telegraph

Flight Sergeant Will Barrow was crouched low, his heart pounding, in the belly of a Viking armoured vehicle under intense Taliban gunfire, when a clear and sudden understanding of his own mortality came to him.

But he had one immediate comfort: "I knew that if I died tonight, I would not be alone, because my best pal would be watching over me."

It was at moments like this, as the bullets flew, that Sgt Barrow realised the true value of Buster, the trusty springer spaniel whose job was to protect the troops fighting the bloody war in Afghanistan.

Buster is no ordinary animal but a highly trained arms and explosives detection dog with five military campaign medals to his name, who has saved a thousand lives in Bosnia, Iraq and Afghanistan.

And to Sgt Barrow, his handler, he was also a best friend during times of terror.

RAF Police Sergeant Barrow, a career security forces man, is no softie. Almost 6ft tall, with rugged features and the steely core of a military professional, he has also served in Bosnia, Iraq, the Falkland Islands and Northern Ireland.

But as Buster saved him and his colleagues time and again from deadly explosives, an enduring bond developed between the pair.

Their friendship dates back to their Afghanistan tour. It was 2007 and Buster had been deployed with Sgt Barrow to serve in the desert and poppy fields of Helmand and the slums of Lashkar Gah.

It was a treacherous point in the war, when roadside bombs – improvised explosive devices, or IEDS – and suicide missions were commonplace and the body count of British soldiers was rapidly climbing.

Conditions in the troops' desert camp were basic: food consisted of boil-in-the-bag ration packs, the "mozzipods" they slept in were cramped, and sand permeated everything.

But for Sgt Barrow, 48, at least there was Buster.

In the book he has written as a tribute to their partnership, he recalls the dog's greatest triumph: a house raid in which he tracked down suicide vests primed for detonation. Two bomb-makers and two teenage would-be bombers were arrested as a result.

But Buster's ability to track Taliban insurgents and sniff out bombs were just one aspect of his armoury.

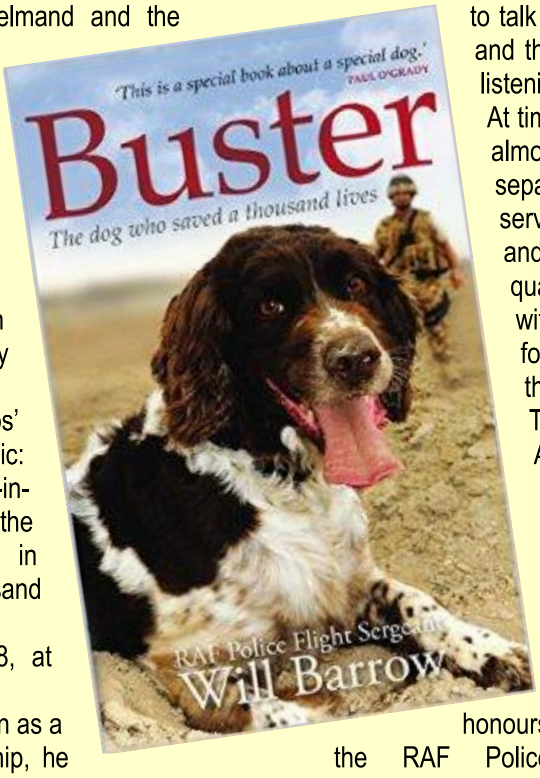
Sgt Barrow recounts how Buster became a diplomatic tool, too: "As we searched and chatted to the locals, we soon had a long train of children in tow – like a canine Pied Piper, Buster drew in his crowd and entertained them," he writes. "Anyone looking on would have wondered how on earth a spaniel from the UK could do so much for the 'hearts and minds' operation."

He was, moreover, a model of calmness in terrifying situations, taking his handler's mind off the immediate risks to himself.

"My main concern was always the little fella, because if he had been injured, my role was non-existent," he says. "As much as I relied on him not to walk us into IEDs, he needed me to feed and water him."

He was also an invaluable comfort, emotionally, to both his handler and his comrades.

Sgt Barrow writes of one evening after coming under insurgent fire: "I was missing home and [my wife] Tracy but when he settled on my chest, I curled my arms around him. I needed to talk about the bad day at work, and this time Buster was the one listening."


'This is a special book about a special dog.'
PAUL O'GRADY
Buster
The dog who saved a thousand lives
RAF Police Flight Sergeant
Will Barrow

At times, Sgt Barrow's tale reads almost like a love story: the separations – when the serviceman flies home on leave and the springer spaniel is quarantined – are poignant, with the spaniel gazing forlornly after his handler as the latter walks away.

Their joint tour of duty in Afghanistan over in 2008, Buster went on to do four more months in Iraq in 2009. Then Buster found a home with Sgt Barrow in Lincoln.

He retired in 2011, aged seven, and a stream of honours followed. He was made the RAF Police's lifetime mascot – unprecedented for any dog – and he has received more requests for television appearances than many human war heroes.

Sgt Barrow, meanwhile, went on to become head of police at RAF Henlow. Looking back at his tours with Buster, he is phlegmatic about the life-or-death situations he faced.

"I don't think we see it the same way as civilians do," he says. "We deal with it, and just get on with things."

Nor does he talk much about the horrors of war. "You don't want to dwell on those sorts of things. It could tip you over the edge a bit."

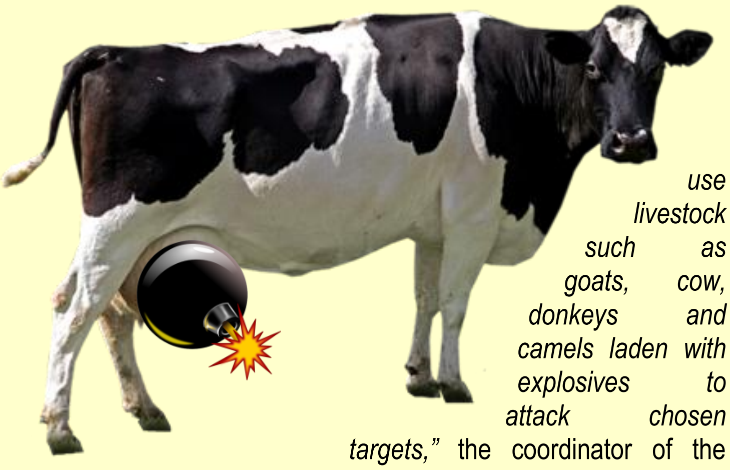
But whatever hardships life throws at him, Buster remains by his side.

"We made a pact from the start to look after each other, and Buster has stayed true to our bargain," he writes. "He saved my life every day we were together. I owe him so much that I can never repay the debt, even if we lived for ever."

Boko Haram to use cows, goats and cobblers to stage attacks

Source: http://rt.com/news/227947-boko-haram-cow-bombs/

Boko Haram insurgents plan to use goats and cows as bomb couriers to carry out deadly attacks, in addition to a new batch of disguised suicide bombers, a spokesperson for the Nigerian federal government warned.



"There is indication of a plan by this group to use livestock such as goats, cow, donkeys and camels laden with explosives to attack chosen targets," the coordinator of the National Information Center Mike Omeri said during a press briefing on Thursday.

Omeri cautioned owners of livestock against taking their animals into city centers in order to avoid being mistaken for militant operatives.

"Persons who rear goats and cows in the center are advised in their own interest to restrict such movements because actions could be taken, and nobody should blame the police and other security agencies for taking the necessary steps," he said.

Reports of seized livestock had surfaced earlier this week when Nigerian press reported that the militants used more than 5,000 cows as a shield during clashes with federal troops in Monguno last Sunday.

"They hide themselves behind the cows and were advancing towards us. All our gun shots were hitting the cows," a soldier who wished to remain anonymous told Nigeria's The Nation.

The intelligence coordinator also suggested that the extremist Sunni group intends to use suicide bombers dressed as cobblers hiding explosives in their toolboxes and striking busy areas.

"Available intelligence reports indicate a plan by Boko Haram to use young ***male suicide bombers disguised as cobblers to hide explosives in their toolboxes*** *and detonate them in soft areas such as markets, restaurants, ATM locations, political rallies, worship centers as well as other public places."*

Omeri advised Nigerians to be vigilant and report any suspicious activity to the police.

Some 1.6 million Nigerians have been displaced, and thousands have been killed as a result of Boko Haram's deadly attacks. Earlier this month the group, which purports to have links to al-Qaeda, massacred more than 2,000 people in the northeastern town of Baga.

EDITOR'S COMMENT: It seems that somebody outthere studies history: Odysseus used sheep coverage to escape Polyphemus one-eye giant! (son of Poseidon and Thoosa in Greek mythology, one of the Cyclopes described in Odyssey)

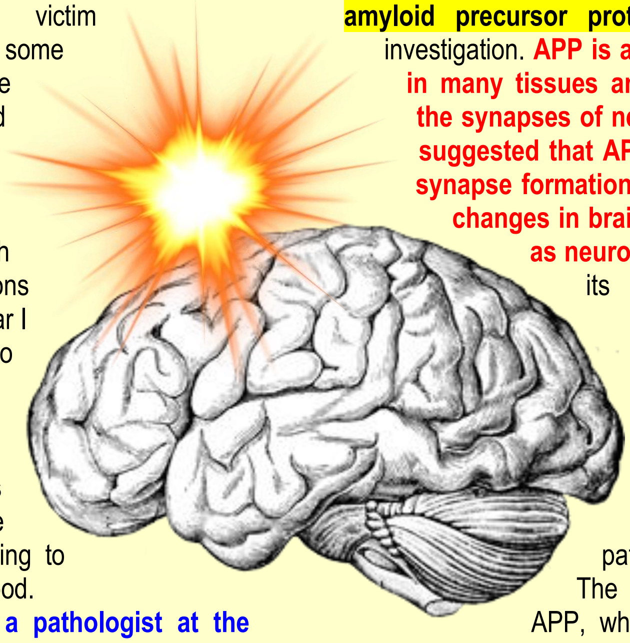
Hopkins investigates IEDs' effects on brain

Source: http://counteriedreport.com/news/hopkins-investigates-ieds%E2%80%99-effects-on-brain

The structure and functions of the brain are highly complex, and in turn, the way it reacts to injury and insults can be perplexing. In fact, it is arguably the most complex and least understood structure in nature.

Researchers at the Johns Hopkins School of Medicine have recently published some interesting and startling findings on the pathological effects observed in the brains of soldiers exposed to improvised explosive devices (IEDs).

An IED, a common weapon of choice for terrorists and insurgents, is a homemade device designed to cause death or injury by using explosives alone or in combination with chemical or biological toxins or radioactive materials. IEDs are hidden to avoid detection and improve effectiveness. Most are activated when the victim interacts with them in some way. Currently, IEDs are employed in Iraq and Afghanistan.



Bomb-induced brain damage is far from a new occurrence, with documented observations as far back as World War I when it was referred to as "shell shock." It is only with the recent advent of modern technology that this type of damage to the human brain is beginning to be studied and understood.

Vassilis Koliatsos is a pathologist at the School of Medicine. Koliatsos and his team have recently published their discovery that **IEDs may cause a unique injury**. According t o their report, **soldiers who have survived an IED explosion may experience yet-to-be-revealed injuries to their brains that may cause social and psychological issues that manifest after they return home. Common side effects suffered by the veterans are depression, anxiety, post-traumatic stress disorder, adjustment disorder and substance abuse.**

According to Koliatsos, examining the brain is like examining the life history of an individual. In the brains of veterans who experienced an IED explosion and later died, researchers observed specific pathological features that may be unique to these victims. Where these lesions occur and the extent of the damage that appears may be a clue to explaining the difficulties that some soldiers experience when trying to readjust to their former lives returning from duty.

Koliatsos and his colleagues studied amyloid precursor protein (APP) in this investigation. **APP is a protein expressed in many tissues and concentrated in the synapses of neurons. It has been suggested that APP is a regulator of synapse formation and is involved in changes in brain structure, known as neuroplasticity.** However, its major function is presently unknown. It has also been implicated in the formation of the plaques found in the brains of Alzheimer's disease patients.

The researchers tracked APP, which routinely travels between nerve cells through an axon. **When an axon is broken by a traumatic injury, APP cannot travel past the break, forming a build-up that induces swelling. Swelling can occur due to numerous forms of trauma; however, the type swelling produced in the brains of IED blast survivors was unique and was found in a honeycomb pattern adjacent to blood vessels.**

These lesions were observed in various regions in the brains, including areas that are involved in memory, decision making and reasoning. They may have been remnants of normal nerve fibers that were broken at the time of the explosion or weakened fibers that were broken by some subsequent insult to the brain. The discovery of these lesions may eventually help in the treatment of soldiers who return traumatized from combat.

Afghans live in peril among unexploded NATO bombs that litter countryside

Source: http://www.theguardian.com/world/2015/jan/29/afghans-lives-in-peril-unexploded-bombs

Jan 29 – International troops pulling out of Afghanistan have left behind a lethal legacy of unexploded bombs and shells that are killing and maiming people at a rate of more than one a day. The vast majority are children.

Bombs dropped from the air coupled with munitions left behind in makeshift firing ranges in rural Afghanistan have made parts of the countryside perilous for locals who are used to working the land for subsistence and raw materials.

Since 2001, the coalition has dropped about 20,000 tonnes of ammunition over Afghanistan. Experts say about 10% of munitions do not detonate: some malfunction, others land on sandy ground. Foreign soldiers have also used valleys, fields and dry riverbeds as firing ranges and left them peppered with undetonated ammunition.

A worker from the Organisation for Mine Clarence and Afghan Rehabilitation teaches mine and unexploded ordnance awareness to a class of children on the outskirts of Kabul. Photograph: Ahmad Masood / Reuters/Reuters

Statistics from the UN-backed Mine Action Coordination Centre of Afghanistan (Macca) show there were 369 casualties in the past year, including 89 deaths. The rate rose significantly in October and November when 93 people were injured, 84 of them children. Twenty died.

Two of those were 10-year-old Mohammad Yunus and his eight-year-old sister, Sahar Bibi. The grenades that killed Mohammad and Sahar, as they were combing through dry branches to collect firewood for their family, should have detonated long before they were picked up. Instead, the shells exploded in the children's hands and ripped through their bodies, killing them instantly. The blasts also injured their two brothers, aged five and 12.

The four siblings were gathering wood about a kilometre from Camp Clark, a US military base in the eastern province of Khost, in an area used by US soldiers for battlefield training. But the grounds were unmarked, said the children's father, Sheren Totakhail, who didn't realise the danger.

In rural areas, children often bring in vital income to households, but collecting scrap metal or herding animals can be fraught with unpredictable risks. Of all Afghans killed and maimed by unexploded ordnance, 75% are children, according to Macca.

"I wish I hadn't had to ask my children to work, but we are a poor family," said Totakhail. "Now, I don't even allow my other children to go to the bazaar for shopping."

Despite the removal of 16.5m items since mine-clearing programmes were established in 1989 after the Soviet withdrawal, Macca and its predecessors have recorded 22,000 casualties in the same period. Unexploded ordnance still kills and injures about 40 people each month. Since 2010, MACCA has recorded 36 deaths from unexploded ammunition on NATO firing ranges alone. The true number is thought to be much higher.

The withdrawal of western troops presents an opportunity to clean the mess up. At the end of the year, Nato's International Security Assistance Force mission was replaced with a training and assistance under the name Resolute Support, which will see much fewer foreign troops on the battlefields.

Though first steps have been taken to tackle unexploded ordnance (UXO), agencies complain the US-led forces are withholding information about where they may have dropped explosives.

"We ask for information about battlefields that may have UXO, but we have received coordinates for only 300 locations. It's not enough," said Mohammad Sediq Rashid, director of Macca.

Colonel Calvin Hudson, Nato's Combined Joint Task Force chief engineer in Kabul, says Nato gives as much information to mine-clearing agencies as possible without compromising operational operational security – coordinates for areas where Afghan forces continue their operations are withheld.

Much of the fighting in Afghanistan has taken place in and around residential areas, increasing the risk of civilian casualties in the aftermath of the war. UK and US diplomats emphasise that international law does not give their countries a responsibility to clear battlefields. But that does not absolve Nato countries of their duty to clean up after themselves, said Rashid.

"It is a moral responsibility," he said, adding that scattering unstable explosives around the country defeats the initial purpose of the war. "Military intervention is the last resort, and it's intended to protect people and stabilise the country," he said.

According to officials in Afghanistan, western governments became more aware of the risks of unexploded ammunition after a spate of accidents, and subsequent critical media reports, in 2013.

The UK and US governments have since planned a survey with UN agencies to detect and clear explosive remnants of war in Helmand. The US has also allocated $500,000 (£330,000) to survey 19 districts around the country that have seen high military activity over the past 13 years. According to a US embassy spokesperson, there are 185 districts with more than 50 "kinetic engagements".

International forces have been more forthcoming when it comes to cleaning up firing ranges. A diplomat at the British embassy in Kabul says the UK and US are planning to share the cost of clearing six abandoned firing ranges outside Camp Bastion in Helmand.

Of the 240 firing ranges around the country used by Nato, 140 are now controlled by Afghan security forces, and will not be cleared yet, including the range outside Camp Clark. The rest have been slated for clearance.

According to Hudson, cooperation between international forces, UN agencies and local organisations has improved. He said the relationship used to be dysfunctional and lack transparency, but now partners meet regularly and are "committed to getting the job done".

Hudson said Nato's firing ranges are due to be cleared by the end of 2015. But because many contaminated areas are still besieged by conflict, the work could be delayed. In December, insurgents in Helmand killed 12 Afghan deminers, reminding international donors that clearing explosives is fraught with danger in more ways than one.

However, despite "the tragic attack on contractor personnel undertaking the task," the British embassy official said, "our commitment to clearing our ranges remains."

While those efforts get under way, the hazards of UXO persist, even in Afghanistan's safest areas. Last February, in the peaceful highlands of Bamiyan, Sajad Ali, 18, and his brother Abdul Khaleq, 16, walked to a dry riverbed to collect firewood. They were unaware New Zealand's provincial reconstruction team had previously used this area for target practice.

While the boys rummaged through a thicket of branches, their donkey ran around on the hillside above. As it went, it kicked a stone down the slope towards the boys, which hit and detonated an unexploded shell, spraying them with shrapnel.

Sajad Ali still has pieces of the shell lodged in his leg and arm, and a long operation scar down his stomach. His brother also survived, albeit with a serious injury in his back. A scrawny boy with jet-black hair, Sajad Ali has lost half the strength in his arm, he said in an interview in the autumn. Now 19, he has developed a stutter from the shock of the explosion, and is afraid to leave the house.

Rashid said the sooner the international community expands its clearance efforts beyond firing ranges and a few other areas, the better. “We think every battlefield needs to be checked,” he said. “Every village and every valley can be contaminated.”

Airlines get more than 50 online threats since Jan. 17

Source: http://edition.cnn.com/2015/01/28/politics/airlines-online-threats-50/index.html

There has been a spike in online threats made against airlines since Jan. 17, when a bomb threat was made against a flight between Atlanta and Raleigh, according to a U.S. official.

Since that threat, authorities have received more than 50 threats made online against airlines. The official says most of the incidents are believed to be copycat incidents.

None of the threats have proven credible. The official, as well as other government officials CNN spoke with on Wednesday, point to the publicity these threats receive for the increase.

"We are continuing to investigate these threats with our law enforcement and airline partners as we do with all stated threats," an FBI spokesman told CNN on Wednesday. "Threats of this nature can and do result in costly responses from a multitude of law enforcement and airport entities and greatly inconvenience travelers. Individuals responsible can be prosecuted federally."

On Jan. 17, F-16 fighter jets were called in to escort two passenger planes into Atlanta's Hartsfield-Jackson International Airport after a bomb threat made on Twitter was deemed credible, according to military officials.

Southwest Airlines Flight 2492 and Delta Flight 1156 landed safely at the airport and were searched by bomb disposal units, according to airline officials. Nothing out of the ordinary was found, officials said.

One runway was closed temporarily, causing delays for other flights as passengers on the two flights were questioned and their luggage was searched by bomb-sniffing dogs, officials said.

The Hidden Problem That Kills 15,000 People Every Year

By Beenish Ahmed

Source: http://thinkprogress.org/world/2015/01/30/3617554/landmines/

Somayeh lost her right leg when she was 13 years old and the car she was traveling in hit a landmine. CREDIT: AP

In an age of shooting sprees and suicide bombings, landmines seem a distant threat. But in the last week alone, seven people were killed when they came into contact with the explosive devices: an 11-year-old boy in Egypt’s Sinai Peninsula, one person in the disputed territory of Western Sahara, and at least five were killed in Paksitan's Balochistan province. Often decades old, landmines litter the terrain of resolved conflicts and pose continuing threats to those who live in their midst.

According to the United Nations, there are 110 million land mines still buried in the ground — and more than 15,000 people are killed by landmines every year.

There are an estimated 110 million land mines buried in the world -- waiting for their next victims.
source: http://www.unicef.org/sowc96/9ldmines.htm
THINKPROGRESS

Fadil Mustafa and his family fled their village when ISIS moved in on Kobane last fall. But with their backs to the militant group, they faced an unexpected threat.

"As we crossed [into Turkey]," the 13-year-old told Al-Jazeera, "A mine exploded under my brother and me. My brother was killed. I lost my legs."

Turkey signed the Mine Ban Treaty in 2003 but has been slow to begin the expensive and painstaking task of clearing mines. To make matters worse, Human Rights Watch believes that Syria has planted landmines along its borders with Turkey and also Lebanon.

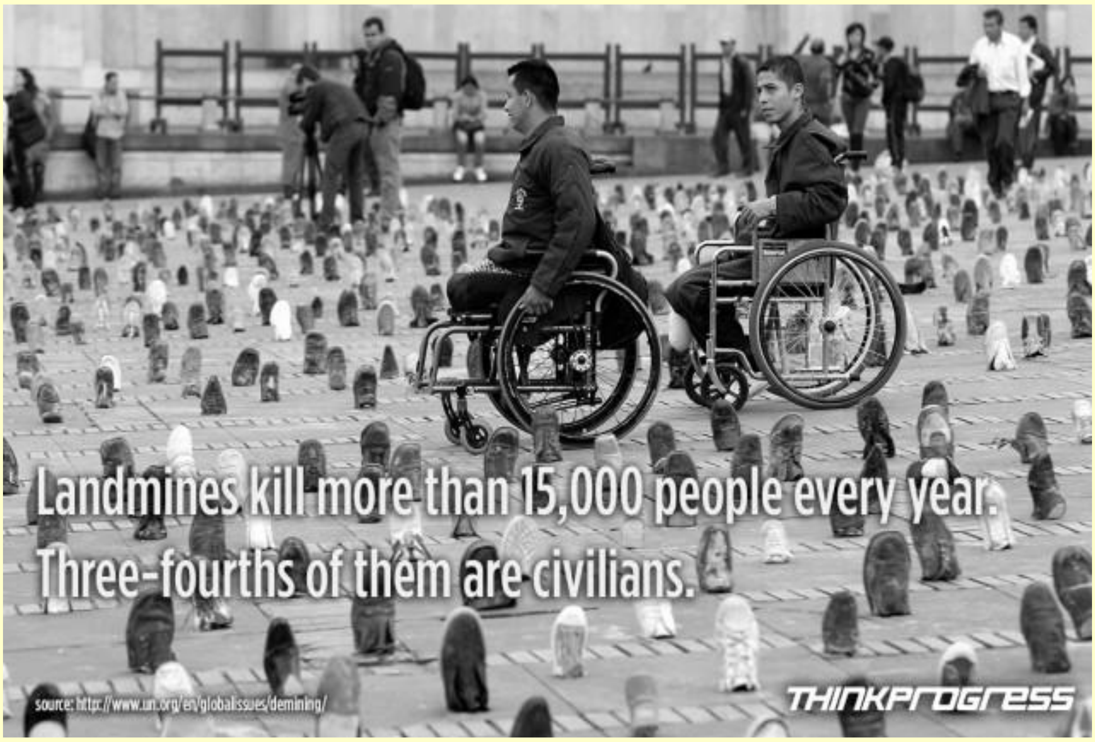
It can cost up to $1000 to clear a single mine, according to the Halo Trust, a charitable organization that has committed to clearing mines around the world for the last 25 years. The organization recently released a report on its work to rid the world of landmines which not only pose grave risks to people's lives – but also to their livelihoods.

It costs anywhere from $300 to $1000 to deactivate & clear a single mine.
source: http://www.un.org/en/globalissues/demining/
THINKPROGRESS

"We destroyed several MON-200s here," Daniel Antonio said referring to Soviet-made mines which each contain 26 pounds of explosives.

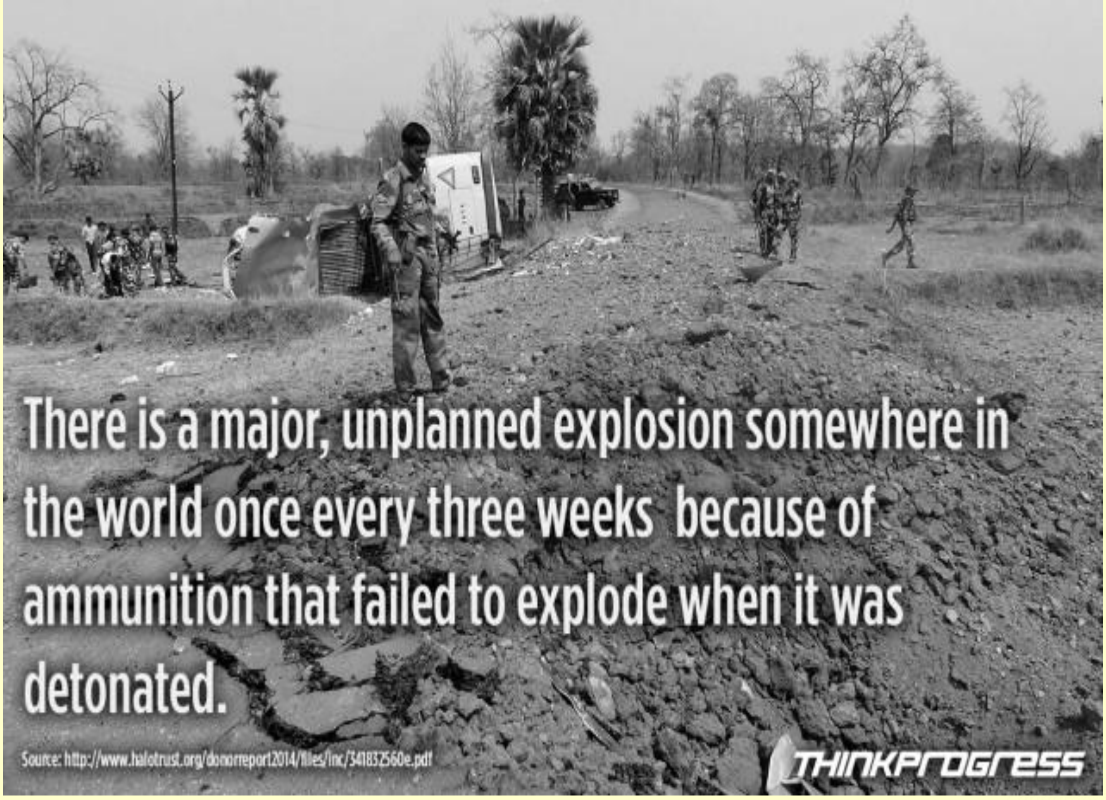
Antonio worked with Halo to help clear a plot of land in southern Angola that belonged, in part, to his grandfather. His work has helped his own family and others in the area to be able to plant crops there without fear, increasing their incomes and their quality of life.

The Halo Trust has destroyed 86,000 mines in Angola, a country dotted with them as a result of a 27-year long civil war that ended in 2002. The West African nation signed on to the United Nation chartered Mine Ban Treaty that same year.


Landmines kill more than 15,000 people every year.
Three-fourths of them are civilians.
source: http://www.un.org/en/globalissues/demining/
THINKPROGRESS

But many countries, however, including China, India, Pakistan, and the United States have refused to sign the Mine Ban treaty. Five non-signers – Israel, Libya, Myanmar, Russia, and Syria – have used landmines since 2009.

Here are some more facts about the hidden – but very real danger – of landmines:


There is a major, unplanned explosion somewhere in the world once every three weeks because of ammunition that failed to explode when it was detonated.
Source: http://www.halotrust.org/donorreport2014/files/inc/341832560e.pdf
THINKPROGRESS

One in 235 Cambodians have been the victims of landmines and explosive remnants.
Source: http://www.halotrust.org/donorreport2014/files/inc/341832560e.pdf
THINKPROGRESS

The United States declared Kosovo 'mine free' in 2001, but the Halo Fund has cleared more than 4,500 mines since then.
Source: http://www.halotrust.org/donorreport2014/files/inc/341832560e.pdf
THINKPROGRESS

All photos crdit: AP/Dylan Petrohilos

__Beenish Ahmed__ is the World Reporter at ThinkProgress. Previously, she was a freelance journalist and Pulitzer Center on Crises Reporting grantee in Pakistan. She is also a former NPR Kroc Fellow. Beenish earned an MPhil in Modern South Asian Studies from the University of Cambridge as a Fulbright Scholar to the United Kingdom and a B.A. from the University of Michigan. Her work has been featured online for The Atlantic, VICE, Foreign Policy, The Daily Beast, The American Prospect, *GlobalPost and on air for NPR, PRI's The World, Deutsche Welle, Radio France Internationale, and Sky News.*

▶ **Read also the 2014 HALO Report:** http://www.halotrust.org/donorreport2014/

HRH Prince Harry with Teresa Heinz Kerry and US Senator Patrick Leahy at a dinner to celebrate his work with HALO in Washington, DC

Celebrating 25 Years of Getting Mines out of the Ground

In 2013 HALO marked a quarter of a century of work removing the deadly debris of war. We held a special 25th Anniversary Appeal with our Patron, His Royal Highness Prince Harry, to raise awareness of the need to employ more deminers to get more landmines out of the ground more quickly.

Throughout the year we held a series of international events and exhibitions. Prince Harry launched our 25th Anniversary Photo Exhibition on Capitol Hill in Washington, DC where he was hosted by Senator John McCain and his wife Cindy, a HALO Trustee. The exhibition portrays the devastating effect of landmines, our work to remove them and the positive impact demining has on communities. The exhibition then travelled to Sri Lanka, Kosovo, Colombia, Mozambique, San Francisco and Google's campus in Mountain View.

Prince Harry also visited our demining operations in Angola, following in the footsteps of his mother, Princess Diana, who visited a minefield in Angola in 1997. It gave the Prince an opportunity to meet with HALO deminers and beneficiaries, while bringing worldwide media attention to the ongoing landmine problem.

Speaking at a dinner in Washington, DC hosted by the British Ambassador Sir Peter Westmacott to recognise Prince Harry's work with HALO, the Prince recalled his mother's interest in the issue and paid tribute to HALO and our donors:

"My mother, who believed passionately in this cause, would be proud of my association with HALO. In her special way, she adopted it as her own. She would join me – along with all of you, I'm sure – in praising HALO for the amazing work that it has done over the past quarter century, and in hoping that one day soon its humanitarian work will be done."

Thank you to all our donor governments, foundations and individual supporters for their invaluable support over the last 25 years. We look forward to continuing our work together, "getting mines out of the ground, for good".

Can a handheld device detect IEDs?

Source: http://defensesystems.com/articles/2015/02/09/army-handheld-detectors-for-ieds.aspx?admgarea=DS

In its continuing effort to prevent injuries caused by buried explosives, the Army is looking to put the latest detection technologies into a lightweight handheld device with a user-friendly interface that accommodates data from multiple sensors.

The Army has issued a solicitation looking to collect information in nine areas related to detecting buried explosives, which can include landmines, metallic and non-metallic improvised explosive devices and triggering devices with non-metallic conducting components and wires, the solicitation said.

Those nine areas of interest the Army wants to investigate:

1. New ground penetrating radar antennas designs with a larger detection footprint, deeper detection and better signal-to-noise ratios. And it would have to fit in the smaller package. GPR can look like small tractors, lawnmowers or, in some cases, something you look for coins with at the beach.
2. Electromagnetic induction (EMI) sensor designs capable of detecting the full range of metallic and low-metallic buried explosive hazards components listed above.
3. New methods for detecting wires, possible with alternative sensors that can increase probability of detection of wires over GPR and EMI sensors alone.
4. Integrated solutions for tracking the position of all detection sensors during operation, with accuracy down to a centimeter.
5. User interface display designs that can provide additional information on targets encountered and feedback of sensor responses and position. The Army wants to be able present data from all sensors to the user with both 2D and 3D visual representations on a display that can be mounted or integrated on the detector.
6. Techniques for achieving higher signal-to-noise ratios in sensor components, including techniques to stack signals and incorporate

positioning information to further improve detection localization, target identification, multi-target resolution and clutter discrimination.

7. New detection algorithms making use of enhanced sensor data and positional information to achieve the same goals listed in No. 6.

21st EOD Company Soldiers test high-tech tool

Source: https://www.dvidshub.net/news/154221/21st-eod-company-soldiers-test-high-tech-tool#.VNztHi6TLz4

Soldiers from the 21st Explosive Ordnance Disposal Company (Weapons of Mass Destruction) conducted the first ever test of the liquid abrasive cutter on high explosives at New Mexico Tech's Energetic Material Research and Testing Center Jan. 29.

Soldiers from the 21st Explosive Ordnance Disposal Company (Weapons of Mass Destruction) **conducted the first ever test of the liquid abrasive cutter on high explosives.**

Seven EOD technicians from the Kirtland Air Force Base, New Mexico-based 21st EOD Company remotely cut eight MK84 bombs at New Mexico Tech's Energetic Material Research and Testing Center Jan. 29.

The 21st EOD Company is part of the 242nd EOD Battalion, 71st EOD Group, 20th CBRNE Command (Chemical, Biological, Radiological, Nuclear, Explosives). The Aberdeen Proving Ground, Maryland-based 20th CBRNE Command is the U.S. Defense Department's only multifunctional command that combats CBRNE threats around the world.

"Experiments conducted with the LAC will eventually contribute to the EOD community's understanding of explosive reactions to different dynamic operations," said 21st EOD Company 2nd Platoon Leader 1st Lt. Mark Wiseman.

A native of St. Louis, Wiseman said the 21st EOD Company was selected to test the liquid abrasive cutter because of its relationship with the organization that designed it, the Lawrence Livermore National Laboratory.

Along with Wiseman, the EOD Soldiers involved in the LAC tests were Staff Sgt. Joseph Salmond from Pittsburgh; Staff Sgt. Jason Trahan from Ault, Colorado; Staff Sgt. Michael Laurie from Gloucester, Massachusetts; Staff Sgt. Anthony Dymond from Montclair, California; Sgt. Zachary Pickard from Shakopee, Minnesota; and Spc. Andrew Altonji from Santa Fe, New Mexico.

The seasoned Army EOD team has a total of eight combat deployments.

The Energetic Materials Research and Testing Center and Lawrence Livermore National Laboratory took part in the tests.

Col. Heidi Hoyle, the commander of the Fort Carson, Colorado-based 71st EOD Group, said the experiment could benefit the entire EOD and scientific community.

"This experimental procedure looks to provide the greater EOD and energetics scientific community increased fidelity on water-based cutting operations," said Hoyle.

... 72 BARBIES!?
YOU KIDDING ME!!?
WHAT DO YOU WANT
ME TO DO?...
rodrigo
expresso

JEFF DARCY The PLAIN DEALER ©2010 6/6
TOYOTA
WHAT HAPPENED TO QUALITY CONTROL? MY NISSAN PATHFINDER WOULDN'T EXPLODE!
PAKISTAN TALIBAN

Kaspersky Lab Presents a Forecast for 2045

Source: http://i-hls.com/2015/01/kaspersky-lab-presents-forecast-2045/

2045 / Forecast
KASPERSKY
Robots Everywhere
No More Computers
3D Printing – Fast and Cheap
Mechanical People
Smart Homes
Hyper Intelligence
Technophobia
46℃
10:00
$15
30%

Robots Replacing People, Robots Serving People.

About 30 years ago the personal computer began to make its way into regular use – and it went on to transform society and the way we live our lives. Kaspersky Lab's experts decided to mark that anniversary by looking further into the future and imagining how information technology might develop and change our lives in the new digital realities of 2045, 30 years from now.

Robots Everywhere

Before long it's likely that the world's population will include billions of people and billions of robots, with the latter doing almost all of the heavy, routine labor. People will work on improving the software for the robots and the IT industry will be home to companies developing programs for robots just like they now develop apps for users to download and install.

Mechanical People

To a certain extent the boundaries between robots and humans will become blurred. Transplants will start using electronically controlled artificial organs and prosthesis will be a routine surgical procedure. Nanorobots will travel deep into the body to deliver drugs to diseased cells or perform microsurgery. Specially installed sensors will monitor people's health and transmit their findings into a cloud-based storage that can be accessed by the local doctor. All of this should lead to a considerable increase in life expectancies.

Smart Homes

Moreover, people will live in smart homes where most creature comforts will be fully automated. The software that runs the house will take care of energy, water, food and supplies consumption and replenishment. The residents' only concern will be to ensure there is enough money in their bank accounts to pay the bills.

Hyper Intelligence

Our digital alter egos will finally be fully formed within a single global infrastructure capable of self-regulation and involved in managing life on the planet. The system will operate a bit like today's TOR; the most active and effective users will earn moderator rights. The system will be geared towards distributing resources between people, preventing armed conflict and other humanitarian actions.

3D Printing – Fast and Cheap

It won't just be dreary chores that are consigned to the history books – production of certain items will no longer be needed. Instead 3D printers will enable us to design and create what we need, from household items like dishes and clothes to the building bricks for a future home.

No More Computers

The PC might have started the whole IT boom, but by 2045 we'll probably only see it in museums. To be more precise we will no longer need a single tool for working with data – which is basically all a computer does. There will be an even greater range of smart devices and these different gadgets will steadily take over the functions of today's PCs. For example, financial analysis will be done by a server controlled by the organization concerned using electronic documents, not by an accountant on a personal computer.

Technophobia

Not everyone will be excited by a brave new robotic world, however. New Luddites (19-century workers who opposed the Industrial Revolution and tried to destroy machines) will likely emerge to oppose the development of smart homes, automated lifestyles and robots. The opposition to IT developments will shy away from using smart systems, appliances and robots for certain types of work, and will not have any digital identity.

"The current rate of development in IT makes it difficult to deliver precise predictions about where we will be in a few decades. However, it is clear that every year our technologies will get even smarter and the people who work with them will need to keep up. We can certainly be sure that cybercriminals will continue to make every effort to exploit any new IT advances for their own malicious purposes," said Alexander Gostev, Chief Security Expert at Kaspersky Lab. "But whatever our world looks like in 30 years, we should start improving its comfort, safety and well-being now. Technology is just a tool, and it is entirely up to us whether we use it for good or for evil."

Kazakhstan Declares Some 700 Websites 'Extremist' In 2014

Source: http://www.terrorismwatch.org/2015/01/kazakhstan-declares-some-700-websites.html

The prosecutor general's office in Kazakhstan announced on January 23 that reviews on the Internet during 2014 determined more than 700 websites contained material considered "extremist" and were ordered blocked.

A statement on the Kazakh prosecutor general's website said that in an effort to counter religious extremism and terrorism, **the office had checked more than 100,000 websites in 2014.**

The prosecutor general's office provided information about the sites to Kazakh courts, which found 703 of those sites had contents that were extremist in nature and ordered those sites blocked in Kazakhstan.

Prosecutor general Askhat Daulbaev said some of the sites were blocked even before there was a court decision to back such a move.

Daulbaev said his office had worked with its Russian counterpart during 2014 to locate and block sites with extremist content and added he hoped that cooperation could serve as a model with Kazakhstan's "colleagues close to our borders and further away."

Who are the most notorious hacking groups?

By Sophie Curtis

Source: http://www.telegraph.co.uk/technology/internet-security/11371524/Who-are-the-most-notorious-hacking-groups.html

The hacking group known as Lizard Squad has been making quite a nuisance of itself this week, claiming responsibility for both an attack on the Malaysia Airlines website, that resulted in users being redirected to a page bearing the headline "404 – plane not found", and an alleged DDoS attack on Facebook that temporarily took the website offline.

Facebook has denied being hacked, claiming the 40-minute outage was due to a change that affected its configuration systems. Meanwhile, Malaysia Airlines assured customers and clients that its website had not been hacked, and that only the domain name – www.malaysiaairlines.com – had been temporarily redirected to another site.

So who are Lizard Squad? Are they a group 'hacktivists' with a political or conspiratorial agenda, or simply teenage vandals? Are they really capable of widespread disruption, or are they all talk? And how do they fit into the broader hacking landscape? Here's how Lizard Squad measures up against some of the other notorious hacking collectives.

Lizard Squad

Lizard Squad is a group of hackers that has gained notoriety for attacking a number of major technology companies including Sony, Microsoft and Facebook.

The group first came to the world's attention in August 2014 when it began attacking a range of online games, including *League of Legends* and *Destiny.* This was followed by more high-profile attacks on Sony's Playstation Network and Microsoft's Xbox Live in August and December.

Lizard Squad appears to have a particular vendetta against Sony. In August 2014, for example, Lizard Squad tweeted a threat against an airliner on which Sony's president of online entertainment was travelling. The plane ended up making an emergency landing.

The group also claims to have affiliations with the Islamic State (ISIS). During the Malaysia Airlines website attack, it described itself as the "Cyber Caliphate" (the hacking wing of Islamic State). It also planted the ISIS flag on Sony's servers in August.

While the motivation behind Lizard Squad's attacks may appear to be political, however, the main purpose is to publicise the group's hacking tool, known as Lizard Stresser. It is thought the link to ISIS could therefore be a ploy to get more coverage by the media.

Following the attacks on PSN and Xbox Live in December, authorities in the US and UK carried out a major investigation, resulting in the arrests of a 22-year-old from Twickenham and a teenager from Southport.

Anonymous

Anonymous is perhaps the most notorious of all hacker groups. It is a decentralised online community of tens of thousands of anonymous 'hacktivists', who use their combined computer skills to attack and bring down websites as a form of protest.

The group became known for a series of attacks on government, religious, and corporate websites. It has attacked the Pentagon, threated to take down Facebook, threatened Los Zetas, the Mexican drug cartel, and declared war on Scientology**.**

In 2010, Anonymous launched Operation Payback**,** after several companies including Visa, MasterCard and PayPal refused to process payments to WikiLeaks. It also publicly supported the Occupy Wall Street movement in 2011, attacking the website of the New York Stock Exchange.

Since 2009, dozens of people have been arrested for involvement in Anonymous cyber attacks, in countries including the

US, UK, Australia, the Netherlands, Spain, and Turkey. Anonymous generally protests these prosecutions and describes these individuals as martyrs to the movement.

The group's motto is "We are Anonymous. We are Legion. We do not forgive. We do not forget. Expect us."

LulzSec

LulzSec (an abbreviation of Lulz Security) was originally formed as a spinoff from Anonymous, following the HBGary Federal hack in 2011. It consisted of seven core members, and its motto was: "Laughing at your security since 2011".

The group's first attack was against Fox.com, leaking several passwords, LinkedIn profiles, and the names of 73,000 X Factor contestants. It went on to compromise user accounts from Sony Pictures in 2011, and takes the CIA website offline in the same year.

LulzSec gained attention due to its high profile targets and the taunting messages it posted in the aftermath of its attacks. Some experts characterised its attacks as closer to internet pranks than serious cyber-warfare, but the group itself claimed to be capable of stronger attacks.

In June 2011, LulzSec released a '50 days of lulz' statement, in which it announced the operation was disbanding. However, the group committed another hack against newspapers owned by News Corporation on 18 July, defacing them with false reports regarding the death of Rupert Murdoch.

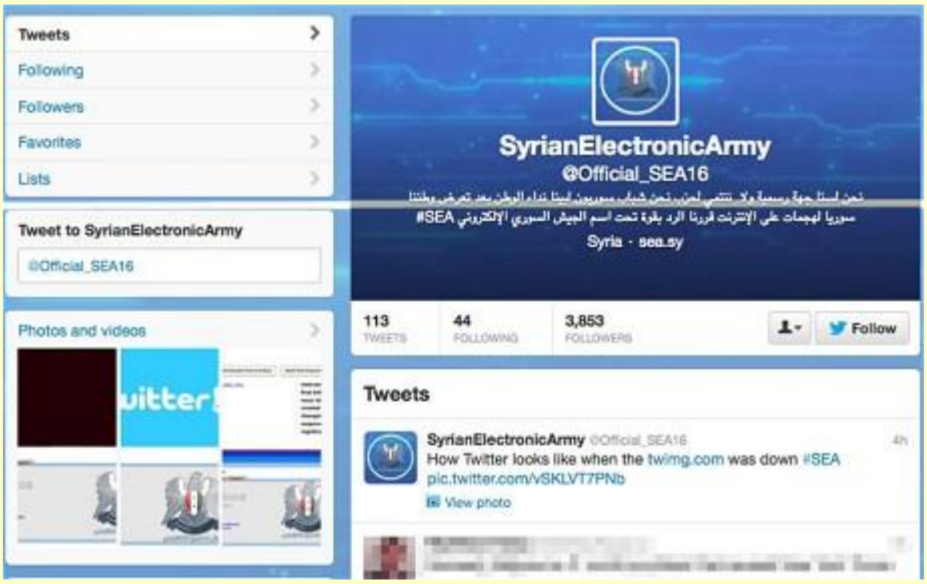
Important members of LulzSec were arrested in 2012 by the FBI, after being turned in by the group's leader Sabu. Prosecutor Sandip Patel said the men lacked the political drive of groups like Anonymous, and saw themselves as "latter-day pirates".

Syrian Electronic Army

The Syrian Electronic Army (SEA) is a group of computer hackers who claim to support the government of Syrian President Bashar al-Assad. It mainly targets political opposition groups and Western websites including news organisations and human rights groups.

The nature of the hacking group's relationship with the Syrian government is unclear. On its website, the SEA describes itself as "a group of enthusiastic Syrian youths who could not stay passive towards the massive distortion of facts about the recent uprising in Syria". However, some experts believe the group is supervised by the Syrian state.

It uses a variety of hacking techniques on its victims, including spamming, defacement, malware, phishing, and denial of service (DDoS) attacks. Often these attacks involve replacing a company's web page with pro-government messages or an image of the Syrian Flag.



SyrianElectronicArmy
@Official_SEA16
نحن لسنا جهة رسمية ولا ننتمي لحزب، نحن شباب سوريون لبينا نداء الوطن بعد تعرض وطننا
سوريا لهجمات على الإنترنت قررنا الرد بقوة تحت اسم الجيش السوري الإلكتروني #SEA
Syria · sea.sy

SyrianElectronicArmy @Official_SEA16 4h
How Twitter looks like when the twimg.com was down #SEA pic.twitter.com/vSKLVT7PNb
View photo

The Facebook pages of President Barack Obama and former French President Nicolas Sarkozy are among those that have been targeted by spam campaigns, as well as the websites and Twitter accounts of a wide range of news organisations and technology companies.

The SEA's tone and style vary widely from the serious and openly political to ironic and humourous statements.

***Sophie Curtis** is a technology reporter at the Daily Telegraph. She previously worked for a number of specialist technology publications including Techworld and eWeek Europe.*

Early warning systems to boost security for critical infrastructures

Source: http://www.homelandsecuritynewswire.com/dr20150129-early-warning-systems-to-boost-security-for-critical-infrastructures

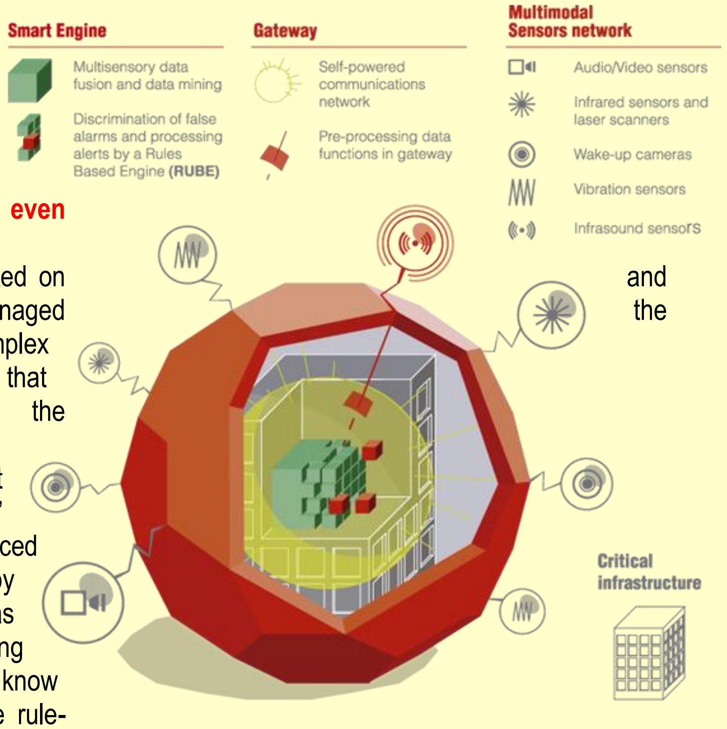
Jan 29 – Our daily lives draw on energy from power stations; we may well use stations and airports; we get our water from reservoirs — all these are known as critical infrastructures. **The EU-funded ARGOS project is developing early warning systems to boost security. The project's innovative approach extends the "security zone," enabling operators to get warning signals as soon as a situation arises. Now the project has produced a 3D video to show how their research can be applied to help our vital infrastructure to become even more secure against intruders.**

CORDIS says that the simulation, posted on YouTube, shows how the project has managed to create a system that uses complex techniques to calculate risk factors that sensors identify outside the installations' perimeter.

Using data mining, data fusion, and what are known as "rule based engines," ARGOS, which stands for Advanced Protection of Critical Buildings by Overhauling Anticipating Systems, has developed an innovative early warning security system, letting site operators know whether there is a potential threat. The rule-based engines allow operators to "teach" the system what alarms are true enabling systems to 'learn' and improve over time.

By bringing together cutting-edge computer science and analytics, the system avoids sounding false alarms which means operators monitoring the warning system know it is not throwing up false positives, such as wild life movements. Responses can be made by operators on site and those managing installations remotely.

Along with creating technology that is able to assess real risk, **ARGOS is also focused on low energy solutions, making it able to operate even in environments in which energy may not always be available.** Researchers have managed this by using energy efficient algorithms, low energy communications and self-powered networks of sensors. Video sensors have auto sleep modes and the microelectronics involved have been optimized for energy efficiency.


Smart Engine
Multisensory data fusion and data mining
Discrimination of false alarms and processing alerts by a Rules Based Engine (RUBE)
Gateway
Self-powered communications network
Pre-processing data functions in gateway
Multimodal Sensors network
Audio/Video sensors
Infrared sensors and laser scanners
Wake-up cameras
Vibration sensors
Infrasound sensors
Critical infrastructure

In bringing the above elements together, researchers have created a system to keep vital installations safe even when they stretch over hundreds of kilometers where no security personnel are available.

The technology can also be used for hydroelectric and harbor installations, to prevent attack from the sea or of cargo ships in harbors. Pipe lines, energy installations, and nuclear reactors will also be able to benefit from the technology and ARGOS can also be used to detect threats from the air. Infrasonic sensors can detect the directions in which vehicles are travelling and infrared cameras and laser scanners have been fine tuned to give reliable data in fog and at night.

The project, which runs from the start of 2014 to the end of 2015, receives €3.5 million of investment under the FP7 program.

▶ **Read more on Argus project at:** http://www.argos-project.eu

Will DPM 5GL Save Cybersecurity?

By Larry Karisny

Source: http://www.govtech.com/dc/articles/Will-DPM-5GL-save-cybersecurity.html

We are at an interesting crossroads in cybersecurity -- somewhere between cyberwar and cybersecurity. There were more attacks than ever in 2014, including the largest state attacks, and in 2015, there are predictions of even more attacks.

All this comes at a time when the largest use of the Internet -- that will dwarf all current Internet use -- will be massively increased by the Internet of Things (IoT) and cloud computing. Both are projecting massive growth in the upcoming year with both having known cyberattack vulnerabilities.

Preparation for inevitable cyberattacks is imminent, and these new technologies will offer increased attack vectors. These attacks occur in microseconds, and only technology that works faster than this can fix it. So what are we doing wrong? And what exactly should we do?

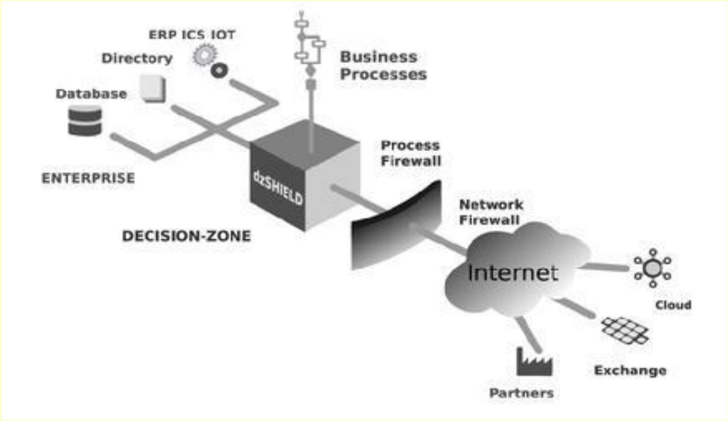
This is where DPM 5GL -- Digital Process Management 5th Generation Programming Language -- comes into play. But what is DPM 5GL? To explain, I must start with some basics.

Doing nothing is not an option

Remember the days when you simply didn't open an unrecognizable executable file as a means of protecting yourself against cyberattacks? Well those day are long over. We live in a time when software has been released with admitted back doors, microchips can have hidden malicious functionality, smartphone apps can actually be used as cyber exploit tools, cloud computing breaches are increasing, and the IoT is web of devices being connected to the network without even being seen by the provider. And as we are increasing the potential of breach with new technologies that have even worse vulnerabilities, we have yet to address *known* cybersecurity vulnerabilities. There will soon be a tipping point of cyber breaches, and all projections point to this year.

But there is a fundamental flaw in all current cybersecurity technologies. They work after the attack has occurred -- but wouldn't it be better to avoid a hack altogether vs receiving notification that your database has been hacked? Would you prefer discovering that your software or chip set is doing something wrong, or would you like real-time validation that it's performing as expected?

At best, current cybersecurity technologies aggregate data that can be historically analyzed in the hopes the problem might be found. This means we are doing little to proactively stop cyberattacks in real time -- and it's why everyone agrees that the cyberattackers will continue to have the advantage. Historical-based cyberattack information technologies are no longer an acceptable option in addressing attacks, as machine actions can occur in microseconds. Cybersecurity must act within microseconds to be effective in securing our information processes. We can no longer use the same current cybersecurity technologies that are, at best, a deterrent, and expect different results. At this point, we are losing ground to cyberattacks.



Assuming You're Always Under Attack

One of the recommendations given by cybersecurity analysts is to assume you've already been attacked. This is one of the concerns I have in current Intrusion Prevention Systems (IPS) cybersecurity technologies and Intrusion Detection System (IDS) cybersecurity technologies.

This assumption validates that current IPS encryption technologies are, at best, a first-level defense in cyberattacks -- and IDS technologies didn't even see the attack come in. With these two valid assumptions (and cybersecurity vendors now admitting to these inefficiencies), we must conclude that our defensive cybersecurity technologies are not enough to stop attacks. If you can't stop attacks, then what?

There have even been discussions on the use of counter attacks as a offensive retaliation -- a disturbing trend being seen in nation state attacks that we should be very careful about. Cyberattack expertise can be bought on the open market with both white hats and black hats offering services. Nation states are actually hiring independents who have little loyalty to the nation or cause, and more interested in the money. Even ex-NSA and Israeli Unit 8200 are leaving their public-sector organizations and going to the private sector for the money.

The fact of the matter is that there are thousands of these people who have the skills to hack their desired targets. They are just doing what they need to do today and not necessarily concerned about the long term outcome of cyberattacks. Whether they are patching known vulnerabilities that were put in by nation state spy organization or a hackers just doing it for fame and fortune, this back and forth hack and patch cyberwar could be devastating. The problem is who wins or gains when this is done. The short answer today is the aggressor wins in the short-term until eventually stopped with some short-term patch. Then a new exploit is found and we start all over again. The problems are these: Who is the aggressor? Who wins? And how much does all this cost? This has led to a whole new field of cyber risk management that unfortunately is more of a guess than a science.

Can we insure cybersecurity?

The short answer as to whether we can insure cybersecurity is no.

The problem with cybersecurity insurance is in these two questions: How much did they take? And how deep was the breach?

Why? Because how can an insurance company calculate a premium or settlement in a cyberattack without complete information? Frankly, the cybersecurity industry doesn't have enough analysts now, so where is the insurance industry going to find the expertise to even evaluate the attack? We don't have enough trained cybersecurity analysts today to even support our current information processes. Even if you are to get a cyber insurance policy, you must prove how well you are currently protected. If current cybersecurity technologies are simply deterrents to cyberattacks, then who would want to insure you in the first place?

As you can see, even a monetary defense posture of cybersecurity insurance is unreasonable. Rather than getting caught up in cyber war offense and defense and patch technologies, we should be looking to cyber intelligent technologies that can authenticate, view, audit, analyze and block these attacks in real time. Who cares about who did it -- when you get robbed, do you want your money back or to know who the robber was? Wouldn't it be better to just not be robbed in the first place? Cyberattacks use offensive technology, and we need to defend these attacks with better proactive defensive technologies. This can be done, but to achieve it, we must be better and faster than the attackers.

5GL DPM closes that hack gap

We currently use software that runs mainly on 3rd Generation Programming Language (3GL) and 4th Generation Programming Language (4GL) technology. To explain what 5th Generation Programming Language is, it's is best to compare it to previous 4th generation programming language.

While fourth-generation programming languages are designed to build specific programs, fifth-generation languages are designed to make the computer solve a given problem -- without the programmer. This way, the programmer only needs to worry about what problems must be solved and what conditions need to be met, without worrying about how to implement a routine or algorithm to solve them.

5GL is a programming language based on solving problems using constraints given to the program, rather than using an algorithm written by a programmer. Most constraint-based and logic programming languages, as well as some declarative languages, are fifth-generation languages.

By adding Digital Process Management to 5GL, you now have a comprehensive real-time intelligent viewing capability during data in motion, which can catch cyberattacks before they occur.

It is important to note that 5GL does not use algorithms. This is a significant departure from current security and analytic technologies that are heavy dependent on algorithms, which, in many cases, are targets for cyberattackers.

A recent whitepaper written by the father of cybersecurity -- M. E. Kabay, professor of Computer Information Systems at the School of Business & Management at Norwich University -- clearly identifies the immediate need for DPM 5GL technology. In the white paper, Kabay states: "Have you ever wondered why computer and network security are so difficult? One of the problems is that it’s really difficult to make sure that all the proper procedures used by machines and by people are in fact in use to protect their information."

Process events are usually locally activated, with the process knowledge being driven by the local operator and the procedures defined both locally and company-wide by thorough standards and proprietary process flows. These human and digital process flows are the heart of every organization that not only determine security breach anomalies, but also the competitive process efficiency and ROI of each organization.

Current 3GL and 4GL programming languages were mainly focused on interconnecting and automating systems rather than intelligently monitoring their operations in real time during data in motion.

Adding to this system complexity is an increasing amount of software and device applications now being connected to the enterprise, cloud or Internet that can affect or even exploit the control system processes. If we are to continually interconnect digital devices and software to our system processes, we must start to manage this digital information. Kabay continues by saying that if a user can develop an unambiguous, complete flow chart of a process, "that chart can be converted into a working program (instructions, or code, for the computers to execute) to identify deviations from the expected operations or data. Computing professionals call the process of turning a design into a working program instantiation.”

By combining DPM and 5GL, they are able authenticate, view, audit and block system events in real time during data in motion across multiple software, hardware and network platforms. Kabay gives specific examples of how 5GL DPM could be used by more than 25 industries verticals.

Another important part of 5GL is that it simplifies current software events while monitoring these process events in microseconds. Today's software is so complex that the complexity itself is where hackers find weaknesses. This is why current patch and pray technologies are having difficulty in just keeping up with attacks. We must be ahead of the attack actions in real time while improving the ability to observe both the correct events and attack anomalies even if using multiple networks and layers of software. 5GL has the unique ability of intelligently recognizing these multiple process events in milliseconds.

In Conclusion

Today's information technologies were really built to automate processes and not necessarily to view or secure the events within the processes. All current IPS and IDS cyber security technologies are not really good at security these events because they frankly don't even see them or know they are an accepted part of the process. There is nothing more important than events in information processing because they represent the exchange of information between systems applications, and the individual and machine actions that initiate them. All systems and applications, enterprise, network, cloud, IoT -- it doesn't matter. If you really watch what hackers do, you can see that they manipulate digital events or software to get their desired results.

The knowledge of this process workflow is local. Your house, the area you live in, your work processes, even your global interaction. If we are to secure these processes, we must define and validate the event flow in real time during data in motion. From giving a key to the office to having access to complex control system processes, event processes are driven locally and are the first step to achieving true cybersecurity. DPM is used to pre-define the sequence of these multiple events in the accepted processes. By adding the intelligence of 5GL to the pre-determined digital management process, we can effectively be ahead of cyberattacks in microseconds rather be in the reactionary cybersecurity mode we are in today.

__Larry Karisny__ is the director of Project Safety.org and a consultant supporting local wireless broadband, smart grid, transportation and security platforms.

Securing the Nation's Ports Against Cyberterrorism

By Leischen Stelter (Editor, In PublicSafety.com)

Source: http://inhomelandsecurity.com/securing-the-nations-ports-against-cyberterrorism/

Ports contribute approximately $3.15 trillion in business activity to the U.S. economy and handle more than 2 billion tons of domestic, import and export cargo annually, according to the American Association of Port Authorities (AAPA). So it is no surprise that physical protection and cybersecurity of ports is a high priority.

Since the Sept. 11 attacks, the government has spent more than $2.5 billion improving the physical security components of ports including: hardening perimeters with fencing, improving surveillance systems, authenticating personnel via the Transportation Workers Identification Credential (TWIC) program, adding sophisticated cargo screening technology, implementing land and sea patrols, and much more.

The U.S. Coast Guard is focusing on hardening ports against cyberattacks. On Jan. 15, the USCG held a maritime cybersecurity standards public meeting to discuss cyber threats to our nation's ports.

"The Coast Guard has a long, proud history of protecting our coasts, our maritime interests and American waters from all manners of hazards and threats. Cybersecurity is one of those threats, and we need to figure out the best way to address those threats," stated Captain Andrew Tucci of the USCG Office of Port & Facility Compliance during the meeting.

Determining how to protect the nation's ports against cyberattacks will continue when officials and academics gather March 2-3 at the Maritime Cyber Security Learning Seminar and Symposium at CCICADA at Rutgers University to discuss cybersecurity risks, threats and counter measures.

The Threat of Cyberattacks on Ports

Ports are especially vulnerable to cyberattacks because their operation—and the operation of ships entering and exiting ports—depends heavily on technology, explained Ernie Hughes, who teaches the Port and Terminal Operations course in the Transportation and Logistics Management master's program at American Military University.

"Throughout the supply chain, nearly all the transportation devices are just big computers and, increasingly, trains, trucks, ships and airplanes are all automated," said Hughes, who has held technology-based positions in companies including Boeing, Tenneco and Getty Oil. "Today a ship largely drives itself using a complex computer system and humans merely monitor things."

Such reliance on technology makes ships and ports extremely vulnerable. Imagine what could happen if a hacker gained control of a cargo ship's navigation system?

Hardening old Systems to new Threats

The dependence on computer systems and technology means that today's ports must harden their networks against cyber threats and face issues updating older technology systems.

"Many of our transportation systems—including those operating ports and ships—were built when the threats were different," said Hughes. Many of these systems were not designed with the sophistication required to keep hackers and other intruders out because they were built at a time when network security was not a requirement.

Even if the government or private business invests money to protect such systems, it can take a long time for such changes to be developed and implemented, adding to the challenge of keeping pace with ever-evolving cyber threats.

It can also be challenging to convince port operators and ship owners that such network enhancements are worth the cost. "Security is a non-functional requirement. It's not something businesses do unless they need to and doing so is based upon the perception of risk," said Hughes. Because an attack has not (publicly) occurred, many operators may not believe upgrading their systems against a cyberattack is worth the high investment.

However, as cyberattacks on private businesses and government agencies continue to make national news, the need to protect the nation's hub of commerce and its economic driver will only become more apparent and urgent.

What Your Facebook Posts Mean to US Special Operations Forces

By Patrick Tucker

Source: http://www.defenseone.com/technology/2015/01/what-your-facebook-posts-mean-us-special-forces/104031/

Jan 29 – It was in the 1873 book **"**On War," that Prussian military scholar **Carl von Clausewitz give birth to the term "fog of war," writing that "war is the realm of uncertainty; three quarters of the factors on which action in war is based are wrapped in a fog of greater or lesser**

uncertainty. A sensitive and discriminating judgment is called for; a skilled intelligence to scent out the truth."

United States Special Operations Command, SOCOM, is trying to dispel some of that fog, moving forward with the development of advanced data mining tools that, if revealed, could make some of the capabilities outlined in documents disclosed by NSA leaker Edward Snowden look quaint.

The utility of social media data is moving quickly beyond simple investigations directly on the battlefield, to that critical moment when a soldier decides whether or not to pull the trigger. According to some military thought leaders, it's law and policy that isn't keeping up.

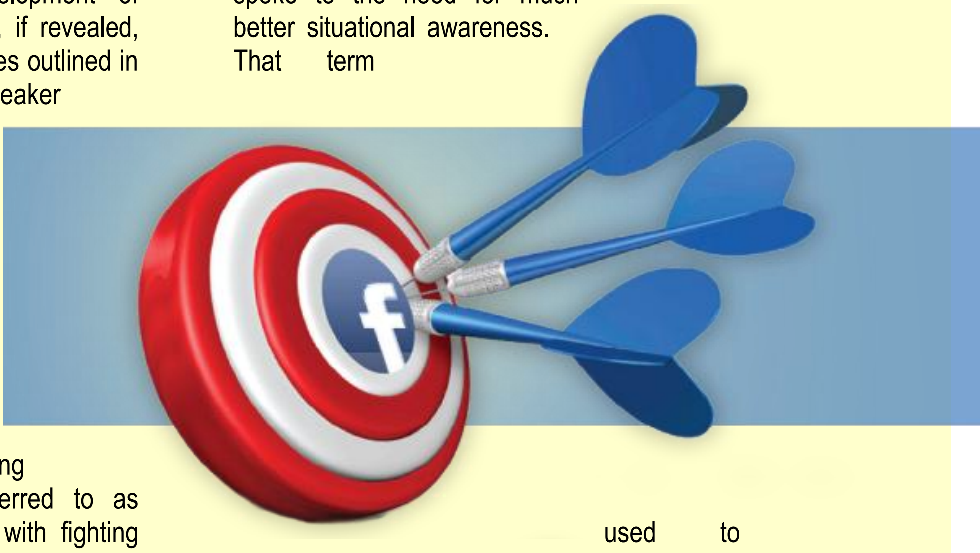
Representatives from elite fighting squads, sometimes broadly referred to as special operations units, tasked with fighting America's most dangerous—and often most secret battles—say that they need better information, including from social networks, to execute missions that take place all over half the globe. That idea may be controversial, and, in fact, many of the tools being developed may never be legal to use. Regardless, according to one of the Defense Department's top lawyers, "Legal uncertainty should not be a barrier to us developing a tool" for use by special operations fighters.

Todd Huntley, the head of the National Security Law Department of the Office of the Judge Advocate General, speaking at a special operations event in Washington, D.C., this week, said that the U.S. should continue to build possibly illegal data mining tools rather than relinquish capabilities.

"We should be very cautious in setting precedent that could limit the development of this technology," he said, adding that if the military waits for the courts before building next generation intelligence capabilities "it will take too long." (He did not say we should actually *use* them outside of law.)

The Defense Department policy that governs the way it collects information on foreign persons, whether for use in combat or just as part of investigations, is called Department of Defense (Instruction) No. 5240 IR. It was originally drafted in 1982. Huntley says that's one reason policy can't keep up with technology or with the battlefield challenges. "If we can't even determine who is and who is not a U.S. person, how do we determine how to use existing policies?"

In a wide-ranging discussion, various special operations thought leaders and key figures spoke to the need for much better situational awareness.



That term used to mean understanding the location of enemies, what arms they might be carrying, etc. Increasingly it means instantaneous data from social networks like Twitter and Facebook to identify of the target in the sniper scope, and who might be connected to him or her.

Stuart Bradin, a retired Army colonel who worked for SOCOM, put it this way: "It would great if we could use social media to Positively ID (PID) someone. Accuracy matters. So social media tools that can help would be a great capability."

In highlighting the most pressing problems that the special operations faces, Anthony Davis, the director of science and technology for SOCOM, highlighted the following: enabling small teams through new cutting-edge gear like the TALOS (also known as the Iron Man suit), developing capabilities to conduct special operations in places like Africa where communication infrastructure is absent; and better support and tools for non-kinetic operators, which primarily means assisting with humanitarian missions but can include gathering intelligence for operational use.

In a previous presentation identifying future needs, Davis highlights data mining and behavior modeling as key to special operation's future.

From that need, new tools are rising. Companies like Snaptrends can immediately connect every

Tweet or Facebook post to a specific location. One satellite image analysis company can, reportedly, link any social media post to point on an incredibly high-resolution map.

But those data mining capabilities are still limited and special operations tools and SOCOM has been looking to build beyond them. In May, the command announced its intent to build a new data-mining tool capable of crawling data from "pre-determined web sites" and to "support geospatial, temporal, relationship, textual, and multi-media visualization and visual analytics" to support "situational awareness in a constrained environment," the a program called Automated Visual Application For Tailored Analytical Reporting, or AVATAR.

As Paul McLeary writes for *Defense News*, the program would "perform link analysis and correlate that information with intelligence that has already been provided by the big U.S. intelligence agencies." That means FBI, NSA and virtually any agency that has useful data. That interoperability in the form a single platform sounds a lot like many of the products developed by Palantir to present and display data across law enforcement agencies to a variety of users. But the AVATAR program shows several critical differences. Most importantly, it would query across government databases and the open web to deliver info to a very specific end user, a special operations fighter who may be using that information in battle.

A Short History of Special Operations Forces Social Network Mining

It isn't the first time that SOCOM has looked into mining social media data for use in operations. **A 2012 project called Quantum Leap** sought to show that open source data, and particularly social media data, could be made useful to active military operations.

The biggest technological outcome of the program was a plug-in piece of software called "Social Bubble," designed by a Santa Rosa company called Creative Radicals. The Quantum Leap report authors describe Social Bubble as "a tool which summons data via the Twitter API to display Twitter users, their geographic location, posted Tweets and related metadata."

According to the authors of the document, the experiment was a success not just in identifying individuals who were actively tweeting and posting but also—and far more importantly for the military—individuals *who happened to be connected to them but who didn't have a social media profile.*

"Overall the experiment was successful in identifying strategies and techniques for exploiting open sources of information, particularly social media. Major lessons learned were the pronounced utility of social media in exploiting human networks, including networks in which individual members actively seek to limit their exposure to the Internet and social media." [Emphasis added.] That's key to developing an ability to deal with an enemy like the Islamic State, where every tweeting sympathizer could be connected to a target who would prefer to stay off the radar.

The end goal of much of this activity is something referred to as "human entity resolution." In the most simple terms, that means figuring out not just the identity of the person visible in the sniper scope but the identities of the people connected to him or her.

Special operations fighters say that information could be critical during an operation. But how much of it can now be obtained quickly and legally? That's become something of a murky issue. The 1982 document aside, not long ago, it was thought to be well settled that law enforcement and the military could use technology to collect information that would otherwise be public (such as your location in a car) and could use data that you gave to third parties like telephone companies. Huntley called those assumptions the basis for a lot of intelligence operations.

"Both of those assumptions have been called into doubt with recent Supreme Court revelations," he said.

The Enemy Is Data Mining, Too

The ability to use social network data operationally is no longer unique to the U.S military. It also represents a growing vulnerability for people in uniform. Mathew Freedman, CEO of the firm Global Impact and a longtime Defense Department advisor, noted, "The digital exhaust issue becomes much more critical…when an airline knows everything you look at on Amazon…through data mining blogs and tweets that you are going to attend future NDIA events." The bottom line for

Freedman: "It will be harder for anyone to be clandestine."

The military is currently testing a new encrypted communications devices that function like smart phone in Honduras. But encryption alone can't solve every potential digital exhaust problem.

Consider the recent hack targeting the Central Command's Twitter and YouTube accounts, which occurred because a Defense Department official did not enable two-factor authentication. The department on Wednesday put out a special instruction document urging employees to take common-sense security precautions. The sheer volume of data we create suggests the invisibility is impossible, both for our enemies and for us. The human race is expected to reach 40 zettabytes of a data a year by 2020, up from 4 zettabytes in 2013. "This is the technological context for every future special operations action," said moderator Klone Kitchen, a special advisor for cyberterrorism and social media at the National Counterterrorism Center.

Because the work of special operations units is so valuable and so very dangerous, special ops fighters occupy a position of some privilege in the military. Republicans, Democrats and politicians every stripe love the idea of small teams of highly talented super warriors doing what it used to require a—very literal—army. And the American people love stories of extreme heroism hence a seemingly unquenchable appetite for Seal Team Six type media

But there's a danger in relying on small teams to do too much, an intellectual trap to which two of the nation's most controversial defense secretaries, Robert McNamara and Donald Rumsfeld fell victim. It may be a behavior that we are repeating.

As McLeary notes, the 2012 White House National Security Strategy "places a premium on the use of special operations forces to operate — quietly — with allies on train and assist missions while continuing their counterterror mission wherever Washington deems fit."

Washington will continue to see fit to send special operations fighters to do a lot more in the coming years. That could include training, equipping, or helping fighters in places like Iraq, Pakistan or Syria. At some point, those fighters may ask, more publicly, for the ability to use controversial intelligence tools to accomplish those missions.

We may not have an answer for them.

***Patrick Tucker** is technology editor for Defense One. He's also the author of The Naked Future: What Happens in a World That Anticipates Your Every Move? (Current, 2014). Previously, Tucker was deputy editor for The Futurist, where he served for nine years. Tucker's writing on emerging technology also has appeared in Slate, The Sun, MIT Technology Review, Wilson Quarterly, The American Legion Magazine, BBC News Magazine and Utne Reader among other publications.*

Is Unrestricted Internet Access a Modern Human Right?

By David Rothkopf

Source: http://foreignpolicy.com/2015/02/02/unrestricted-internet-access-human-rights-technology-constitution/?utm_source=Sailthru&utm_medium=email&utm_term=*Editors+Picks&utm_campaign=COPY_2014_EditorsPicks_Promo+_Russia_DirectRS2%2F2#

National constitutions are supposed to enshrine fundamental rights for everyone — and for generations. Such documents are also products of moments in time and reflect perceptions of life in those moments. That's why the best of them, like the U.S. Constitution, contain the seeds of their own reinvention. Indeed, the secret to a sustainable constitution is that it both captures what is enduring and anticipates the need to change.

Over the years, the U.S. Constitution has been amended 27 times — the first 10 being the Bill of Rights, of course — to ensure that it stays current with prevailing views of what is fundamental or best for the United States. Among the finest examples of the Constitution's adaptability to shifting and maturing norms are the 13th Amendment, which ended slavery, and the 15th and 19th amendments, which guaranteed voting rights for everyone, regardless of race or gender, respectively.

Because it is meant to be malleable, the original Constitution included references to very few technologies. In fact, America's founders were so sure that technologies would evolve over time that they even included protection of the rights of innovators in Article 1, Section 8 (the Copyright Clause). The technologies that were mentioned were ones that by the late 1700s had become so ingrained in day-to-day life that they were seen as natural to the course of human existence, or at least critical to the functioning of government: money, for instance, and a military. In at least two cases in the Bill of Rights, the unfettered use of technologies was seen as necessary for citizens' freedom — those technologies being the press and arms. The press was more than three centuries old when the Constitution enshrined the right to freedom of expression. Meanwhile, the arms referenced were not specified, but no doubt included the firearms of the day that were essential to the upkeep of a militia, which was the express rationale (even if today it is generally overlooked) for the right to bear arms in the first place.

To be sure, technological progress challenges the assumptions that underlie even the best-conceived documents. This has been evident recently in the debate over whether Fourth Amendment guarantees against illegal searches and seizures, which explicitly pertain to the main information technology of the late 1700s ("papers"), cover technologies that have developed subsequently, such as email and metadata. And, surprisingly, there has not been more meaningful debate about whether the Constitution protects the use of arms that Madison & Co. could not possibly have foreseen — namely, modern assault weapons — and how the Second Amendment applies in a world without militias.

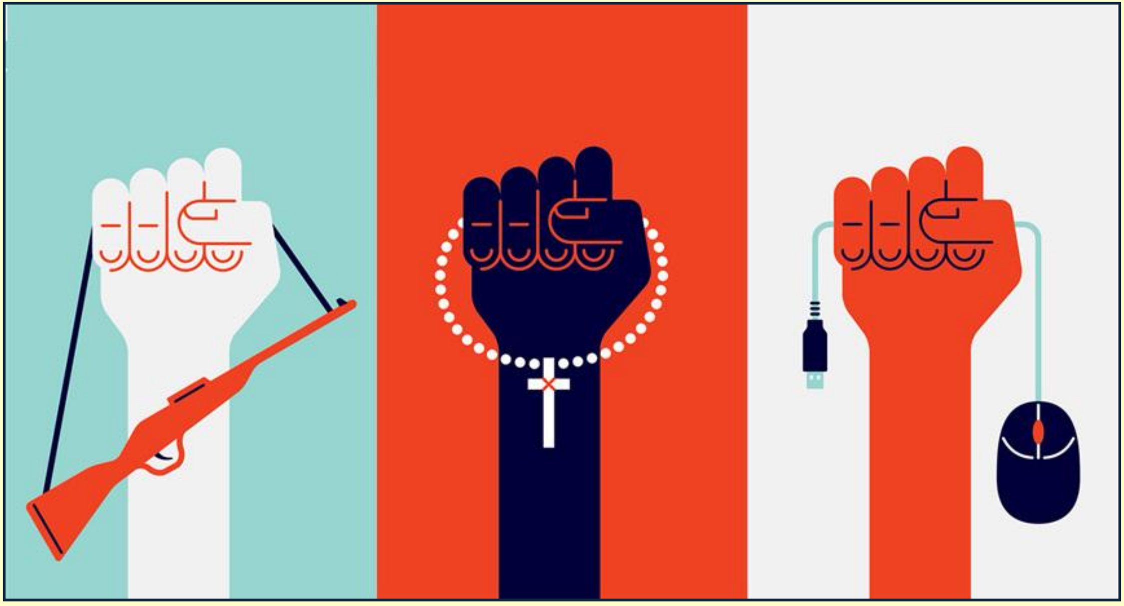


Illustration by Matt Chase

Arguing that people cannot assert rights beyond the imagination of the Constitution's framers is an absurdity, and a dangerous one. As the metadata instance shows, it is hazardous not to bring the American conception of rights in line with the ways and means of modern life. Just as it took the invention of the printing press to trigger a deliberation on freedom of expression, technological changes today are so profound that they demand a reconsideration of what constitutes a fundamental right.

In recent years, more people have maintained that the right to unfettered Internet access is the modern equivalent of the right to the comparable technologies of centuries ago. The U.N. special rapporteur on freedom of opinion and expression has argued that disconnecting people from the Internet constitutes a human rights violation. A number of countries, including Costa Rica, Estonia, Finland, France, Greece, and Spain, have asserted some right of access in their constitutions or legal codes, or via judicial rulings. Meanwhile, some advocates, such as Internet co-inventor Vint Cerf, have argued that content on the Internet must be protected from censorship, lest people's right to information be lost.

The thrust of these arguments converges on a single point: It is difficult, if not impossible in some places, to participate fully in today's world without an open, available Internet. This will become even truer as access is increasingly required to win and perform jobs, gather news, participate in politics, receive education, connect with health-care systems, and engage in basic financial services. (Coin and paper money, one of those few technologies mentioned in the U.S. Constitution, will fade in importance in coming decades, outmoded by mobile banking.)

These are daunting thoughts on a planet on which 4.4 billion people lack Internet access — but that number is shrinking rapidly. The International Telecommunication Union projected in May 2014 that 3 billion people would be online by the end of 2014, up some 300 million from the previous year's projection. In a July 2014 report, based on a canvass of more than 1,400 experts, the Pew Research Center found that even though governments will likely find new ways to restrict Internet access and content, billions more people may be online by 2025. Microsoft has estimated that number will be close to 5 billion.

This revolution carries with it other important questions. If there is a right to the Internet, for instance, does that mean people must also have a right to the electricity needed to plug into the web? The answer, resoundingly, is yes — even though, in a great tragedy of multilateralism, the creators of the Millennium Development Goals failed to set a benchmark for energy access. Electricity once seemed a luxury, but today the nearly 1.3 billion without it are effectively cut off from modern life. Yet this raises another question: In a world where roughly 80 percent of electricity is — and for a long time will be — produced by burning fossil fuels, how is the right to a clean, healthy environment also protected? This points to a need for universal access to clean, sustainable, and affordable energy.

Abstract as a discussion of fundamental rights may seem, determining what people must have to survive and thrive, and wrestling with the conflicts found among these elements, may represent the greatest challenge of this century. The world requires new rules that will empower and enable more and more people to tap into the full promise of human existence, while not simultaneously undercutting and diminishing that promise.

These rules are being made possible by technological advances, but they will not actually come to be if leaders do not act to create them — if governments leave it to the happenstance of progress to sort out tensions among the modern ingredients of life, liberty, and the pursuit of happiness. The conversation about necessary action is already coming too late. The longer it takes to kick into high gear, the longer humans will continue hurtling toward a new economic and social reality. Simultaneously, there will be much slower progress toward ensuring that the gains this reality brings are not offset by the tragedy of too few people benefiting or by the planet's gradual but irreversible degradation.

***David Rothkopf** is CEO and Editor of the FP Group. His latest book, National Insecurity: American Leadership in an Age of Fear was published in October.*

France can now block suspected terrorism websites without a court order

By Amar Toor

Source: http://www.theverge.com/2015/2/9/8003907/france-terrorist-child-pornography-website-law-censorship

Feb 09 – **A new decree that went into effect today allows the French government to block websites accused of promoting terrorism and publishing child pornography, without seeking a court order.**

Under the new rules, published last week by France's Ministry of the Interior, **internet service providers (ISPs) must take down offending websites within 24 hours of**

receiving a government order. French Interior Minister Bernard Cazeneuve says the decree is critical to combatting terrorism, but civil rights groups say it gives the government dangerously broad powers to suppress free speech.

The regulations have been under consideration since 2011, but gained new momentum following last month's terrorist attacks at the Paris office of the satirical magazine *Charlie Hebdo*. The French government has launched a massive anti-terror campaign in the wake of the attacks, countering radical online propaganda with its own anti-jihad website and arresting dozens of suspected terrorism supporters.

Last week, French President François Hollande announced plans to hold major internet companies accountable for sites hosting extremist content, saying the new law would make companies like Facebook and Google "accomplices" to terrorism.

The decree implements two provisions from two laws — an anti-child pornography law passed in 2011 and an anti-terror law passed late last year. A department of the French national police will be responsible for identifying the sites to be blocked, with the suspected terror-related sites subject to review by an anti-terrorism branch. An administrator from the CNIL, France's independent data protection organization, will be charged with overseeing the process.

Once a site is blocked, its page will be replaced with an explanation of why the government took it down. In the case of child pornography pages, the text will also include a recommendation to seek medical help.

Supporters of the measure say it's critical to preventing future attacks, pointing to the growing number of young French nationals who have joined jihadist movements in Iraq and Syria, as well as aggressive online propaganda campaigns from terrorist groups like ISIS.

"Today, 90 percent of those who swing toward terrorist activities within the European Union do so after visiting the internet," Cazneuves told reporters last week, after presenting the decree to French ministers. "We do not combat terrorism if we do not take measures to regulate the internet."

But detractors have criticized the decree for circumventing France's judicial branch, giving the government broader powers to suppress free speech at a time of heightened security concerns.

"In light of the recent arrests that have followed the *Charlie Hebdo* attacks — many of which are clearly overboard — I would say that France's government needs to seriously think about whether this law will stop terrorists, or merely chill speech," Jillian York, of the Electronic Frontier Foundation (EFF), said in an email to *The Verge*.

Others question the effectiveness of the measure. Felix Tréguer, of the French online rights group La Quadrature du Net, says the decree risks "over-blocking perfectly legal content," adding that the domain name system (DNS) blocking that it calls for can be easily circumvented.

"The measure only gives the illusion that the State is acting for our safety," Tréguer said in a statement published today, "while going one step further in undermining fundamental rights online."

***Amar Toor** joined The Verge in April 2012. He previously worked as an editor for Engadget, and before that, as a writer for Switched. He has also worked as a consultant at the OECD in Paris and at Miramax in Santa Monica. He's currently based in Paris.*

EDITOR'S COMMENT: Kind of fed up with these "fundamental rights" and "chill speech" objections. Human lives are above these allegations that are fo no concern to all maintaining websites or blogs that do not pose any threat against society. **It would be a good idea** to have national, European or even international registries were "security websites" would have been registered and approved. Providing information or criticizing what is happening in our world is NOT bad! Recruiting terrorists or giving detailed instruction on how to make a bomb, IS!

Darpa Is Developing a Search Engine for the Dark Web

Source: http://www.wired.com/2015/02/darpa-memex-dark-web/

Feb 02 – A new search engine being developed by Darpa aims to shine a light on the dark web and uncover patterns and relationships in online data to help law enforcement and others track illegal activity.

The project, dubbed Memex, has been in the works for a year and is being developed by 17 different contractor teams who are working with the military's Defense Advanced Research Projects Agency. Google and Bing, with search results influenced by popularity and ranking, are only able to capture approximately five percent of the internet. The goal of Memex is to build a better map of more internet content.

"The main issue we're trying to address is the one-size-fits-all approach to the internet where [search results are] based on consumer advertising and ranking," says Dr. Chris White, the program manager for Memex, who gave a demo of the engine to the *60 Minutes* news program.

To achieve this goal, Memex will not only scrape content from the millions of regular web pages that get ignored by commercial search engines but will also chronicle thousands of sites on the so-called Dark Web—such as sites like the former Silk Road drug emporium that are part of the TOR network's Hidden Services. These sites, which have .onion web addresses, are accessible only through the TOR browser and only to those who know a site's specific address. **Although sites do exist that index some Hidden Services pages—often around a specific topic—and there is even already a search engine called Grams for uncovering sites selling illicit drugs and other contraband, the majority of Hidden Services remain well under the radar.**

White says part of the Memex project is aimed at determining just how much of TOR traffic is related to Hidden Services sites. "The best estimates before were in the single digits—in the one-thousands," he says. "But we think there are, at any given time, between 30,000 and 40,000 Hidden Service Onion sites that have content on them that one could index."

The content on Hidden Services is public—in the sense that it's not password protected—but is not readily accessible through a commercial search engine. "We're trying to move toward an automated mechanism of finding [Hidden Services sites] and making the public content on them accessible," White says. The Darpa team also wants to find a way to better understand the turnover of such sites—the relationships that exist for example between two sites when one goes down and a seemingly unrelated site pops up.

But the creators of Memex don't want just to index content on previously undiscovered sites. They also want to use automated methods to analyze that content in order to uncover hidden relationships that would be useful to law enforcement, the military, and even the private sector. The Memex project currently has eight partners involved in testing and deploying prototypes. White won't say who the partners are but they plan to test the system around various subject areas or domains. The first domain they targeted were sites that appear to be involved in human trafficking. But the same technique could be applied to tracking Ebola outbreaks or "any domain where there is a flood of online content, where you're not going to get it if you do queries one at a time and one link at a time," he says.

In a demo conducted for *60 Minutes*, White's team showed how law enforcement could possibly track the movement of people—both trafficked and traffickers—based on data related to online advertisements for sex. The *60 Minutes* piece wasn't clear about how this was done and appeared to focus on the IP address of where the ads were hosted, implying that tracking where an ad moves from one IP address to another could reveal to law enforcement where the trafficker is located. But White says the IP address is the least important information they analyze. Instead they focus on other data points.

"Sometimes it's a function of IP address, but sometimes it's a function of a phone number or address in the ad or the geolocation of a device that posted the ad," he says. "There are sometimes other artifacts that contribute to location."

For example, an ad attempting to sell the sexual services of a woman or child in one locale might pop up in another location and include a regional address or phone number. White says this kind of data has been used by investigators to find women who were being trafficked.

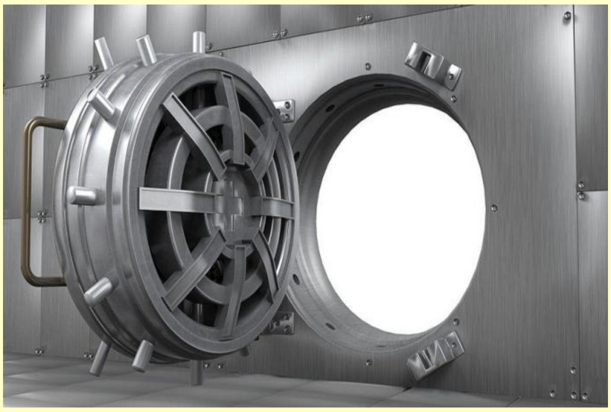
"You can imagine a scenario where people are moving around the country with women and are interested in advertising them—they post ads in different places. It can involve the same women and some of the same info like phone numbers. Via methods of connecting content through shared attributes—meaning the same number or image appearing on ads—you can create a network to understand where these things are connected and where they may be located."

He notes that the connection from the online ads to the real world is not always accurate or a one-to-one match. "But that's why there are investigators and prosecutors involved to do interpretation and make decisions. Darpa just creates the tech, and organizations adopt the technology to use it."

White won't say how much the program is costing, but says it's comparable to other data science projects that have been funded at $10 to $20 million.

The Great Bank Robbery: the Carbanak APT

Source: http://i-hls.com/2015/02/great-bank-robbery-carbanak-apt/?utm_source=Israel+Homeland+Security+%28iHLS%29&utm_campaign=6168e41ebf-Newsletter_English_18_2_2015&utm_medium=email&utm_term=0_8ee2e16ed1-6168e41ebf-87373033&mc_cid=6168e41ebf&mc_eid=521c0e089a



Feb 17 – The story of Carbanak began when a bank from Ukraine asked us to help with a forensic investigation. Money was being mysteriously stolen from ATMs. Our initial thoughts tended towards the Tyupkin malware. However, upon investigating the hard disk of the ATM system we couldn't find anything except a rather odd VPN configuration (the netmask was set to 172.0.0.0).

At this time we regarded it as just another malware attack. Little did we know then that a few months later one of our colleagues would receive a call at 3 a.m. in the middle of the night. On the phone was an account manager, asking us to call a certain number as matter of urgency. The person at the end of the line was the CSO of a Russian bank. One of their systems was alerting that data was being sent from their Domain Controller to the People's Republic of China.

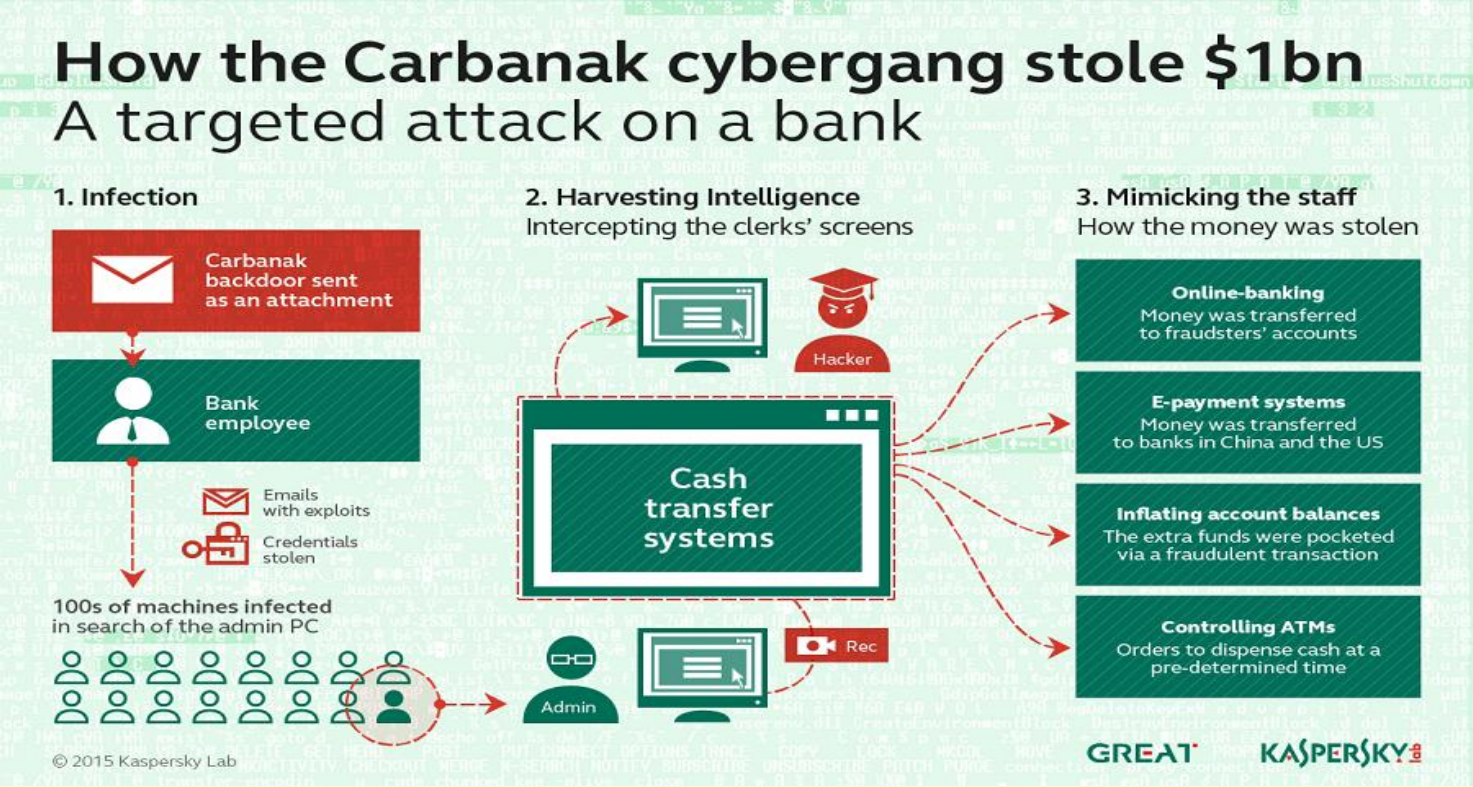
When we arrived on site we were quickly able to find the malware on the system. We wrote a batch script that removed the malware from an infected PC, and ran this script on all the computers at the bank. This was done multiple times until we were sure that all the machines were clean. Of course, samples were saved and through them we encountered the Carbanak malware for the first time.

Modus Operandi

Further forensic analysis took us to the point of initial infection: a spear phishing e-mail with a CPL attachment; although in other cases Word documents exploiting known vulnerabilities were used. After executing the shellcode, a backdoor based on Carberp, is installed on the system. This backdoor is what we know today as Carbanak. It is designed for espionage, data exfiltration and remote control.

Once the attackers are inside the victim´s network, they perform a manual reconnaissance, trying to compromise relevant computers (such as those of administrators') and use lateral movement tools. In short, having gained access, they will jump through the network until they find their point of interest. What this point of interest is, varies according to the attack. What they all have in common, however, is that from this point it is possible to extract money from the infected entity.

The gang behind Carbanak does not necessarily have prior knowledge of the inner workings of each bank targeted, since these vary per organization. So in order to understand how a particular bank operates, infected computers were used to record videos that were then sent to the Command and Control servers. Even though the quality of the videos was relatively poor, they were still good enough for the attackers, armed also with the keylogged data for that particular machine to understand what the victim was doing. This provided them with the knowledge they needed to cash out the money.


How the Carbanak cybergang stole $1bn
A targeted attack on a bank
1. Infection
Carbanak backdoor sent as an attachment
Bank employee
Emails with exploits
Credentials stolen
100s of machines infected in search of the admin PC
Admin
2. Harvesting Intelligence
Intercepting the clerks' screens
Hacker
Cash transfer systems
Rec
3. Mimicking the staff
How the money was stolen
Online-banking
Money was transferred to fraudsters' accounts
E-payment systems
Money was transferred to banks in China and the US
Inflating account balances
The extra funds were pocketed via a fraudulent transaction
Controlling ATMs
Orders to dispense cash at a pre-determined time
© 2015 Kaspersky Lab
GREAT
KASPERSKY lab

Cash out procedures

During our investigation we found several ways of cashing out:

ATMs were instructed remotely to dispense cash without any interaction with the ATM itself, with the cash then collected by mules; the SWIFT network was used to transfer money out of the organization and into criminals' accounts; and databases with account information were altered so that fake accounts could be created with a relatively high balance, with mule services being used to collect the money.

Infections and losses

Since we started investigating this campaign we have worked very closely with the law enforcement agencies (LEAs) tracking the Carbanak group. As a result of this cooperation we know that up to 100 financial institutions have been hit. In at least half of the cases the criminals were able to extract money from the infected institution. Losses per bank range from $2.5 million to approximately $10 million. However, according to information provided by LEAs and the victims themselves, total financial losses could be as a high as $1 billion, making this by far the most successful criminal cyber campaign we have ever seen.

Our investigation began in Ukraine and then moved to Moscow, with most of the victims located in Eastern Europe. However thanks to KSN data and data obtained from the Command and Control servers, we know that Carbanak also targets entities in the USA, Germany and China. Now the group is expanding its operations to new areas. These include Malaysia, Nepal, Kuwait and several regions in Africa, among others.

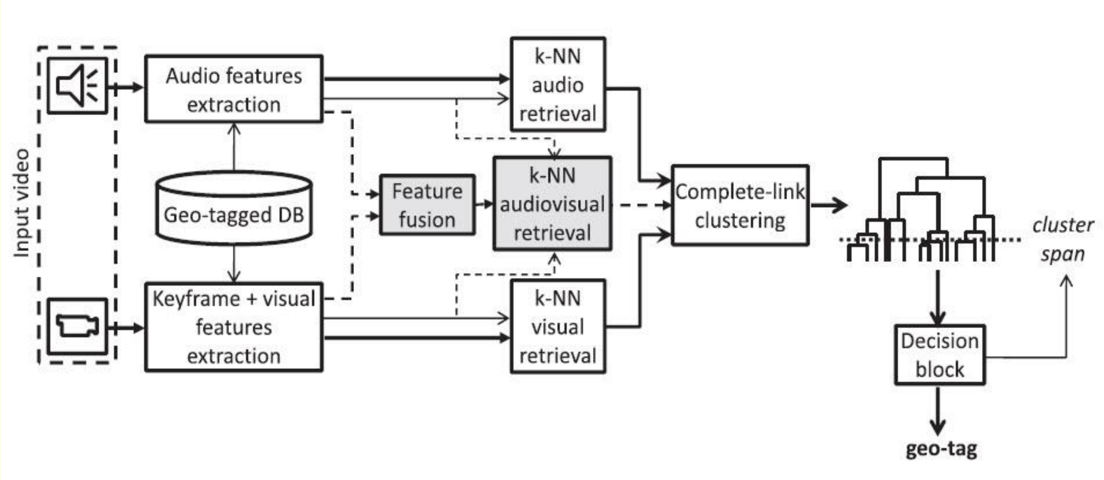
The group is still active, and we urge all financial organizations to carefully scan their networks for the presence of Carbanak. If detected, report the intrusion to law enforcement immediately.

New video technology could help researchers pin-point where Jihadi hostage videos were shot

Source: http://www.independent.co.uk/news/world/middle-east/new-video-technology-could-help-researchers-pinpoint-where-jihadi-hostage-videos-were-shot-10059587.html

Feb 20 – **A new video analysis technology could make it easier for the security services to track down hostages taken by terror groups such as Isis or Al Qaeda.**

The algorithm, developed by researchers at Ramón Llull University in Barcelona, cross-references videos against a huge database of known footage with the aim of matching their locations.



Because terror groups often film and release videos of hostages, the researchers have suggested that the technology could have some counter-terrorism applications.

"Our system does not make any assumptions regarding the location of the videos, but in these cases we are given very valuable additional information to limit the searches, as we already know that we are dealing with the area of Iraq or Syria, and therefore, we would only use reference videos from there," explained Xavier Sevillano, one of the study's authors.

Still in its early stages of development, the technology located 3% of videos included in a recent study to within 10km of their location, and 1% of videos tested to within 1km.

Counter-terrorism researchers and intelligence agencies already employ a series of techniques to 'geolocate' videos – trying to discern the location they were shot.

Eliot Higgins, a research fellow at the Centre of Excellence in Terrorism, Resilience, Intelligence and Organised Crime Research (CENTRIC), has experience in geolocating terror videos.

Mr Higgins told *The Independent* that the technology could be helpful in a limited number of cases but that it would not revolutionise the usually painstaking process.

"To me this seems like interesting technology, and I'd like to see it in action, but I don't think it's going to revolutionise the way geolocation is done," he said.

"In a small number of cases it might make it easier to find a search location, but it seems like those instances where we've located Jihadis to within a few feet of a specific location there's still going to have to be additional work."

He noted that the low success rate of the technology at its early development stage could limit its applications.

Because the technology relies on archive footage, it could also be difficult to use it to geolocate videos shot inside buildings or in remote areas where no archive footage exists.

The latest developments in the technology were outlined in a scientific paper authored by Xavier Sevillano, Xavier Valero, and Francesc Alías called **"Look, listen and find: A purely audiovisual approach to online videos geotagging".**

The paper was published in the most recent issue is the *Information Sciences* journal.

DHS shutdown would have only limited immediate impact on national security

Source: http://www.homelandsecuritynewswire.com/dr20150220-dhs-shutdown-would-have-only-limited-immediate-impact-on-national-security-analysts

Feb 20 – Talk of a halt of DHS operations if Congress does not approve the Republican-proposed DHS funding bill has dominated news and policy circles in recent days. In the Senate, Democrats refuse to pass the House-approved funding bill as long as it contains wording which would defund efforts to carry out the White House's immigration policies, which extends deferred deportation to undocumented immigrants brought illegally to the United States as children (Dreamers) via the Deferred Action for Childhood Arrivals (DACA) and some undocumented parents of U.S. citizens or permanent residents via the Deferred Action for Parents of Americans (DAPA).

Earlier this week, the *Homeland Security News Wire* reported that a federal judge had already placed an injunction on President Barack Obama's immigration efforts. Still Congress has yet to pass the DHS funding bill.

Slate Magazine **explored what would happen if Congress fails to act before the 27 February funding deadline, and found that most DHS operations would continue.** Not approving DHS's $40 billion budget for some time "is obviously not the end of the world," said Representative Matt Salmon (R-Arizona), noting that many agency employees would still report to work through a shutdown.

During the October 2013 government shutdown, 85 percent of DHS employees remained on the job. Just a little over 30,000 of the department's 230,000 employees, mostly in managerial and administrative positions, were furloughed. According to CNN, a Congressional Research Service report says that federal employees "whose work is necessary for the preservation of the safety of human life or the protection of property" would continue to receive pay outside of the appropriations process.

New DHS grants allocated to help states and cities pay for security improvements will, however, be placed on hold, according to a statement from DHS chief Jeh Johnson. Those grants, *Slate* reports, pay for a host of projects including New York City Police Department surveillance cameras, as well as upgrading "obsolete remote video surveillance systems" near the Texas-Mexico border in the Rio Grande Valley. Johnson adds that his department needs a full-year appropriations bill, and not a short-term fix, so it can keep issuing those grants.

Still, a shutdown of DHS via defunding would not put the nation at additional risk. "The reality is that a department shutdown would have a very limited impact on national security," the Yahoo News notes.

U.S. contemplates responses to a cyber-Pearl Harbor attack on critical infrastructure

Source: http://www.homelandsecuritynewswire.com/dr20150220-u-s-contemplates-responses-to-a-cyberpearl-harbor-attack-on-critical-infrastructure

Cybersecurity experts often contemplate how U.S. security agencies would react to a cyber-9/11 or a digital Pearl Harbor, in which a computer attack would unplug the power grid, disable communications lines, empty bank accounts, and result in loss of life.

Summer Fowler is a deputy technical director for cybersecurity solutions at CERT, the U.S. first computer emergency response team, based at Carnegie Mellon University's Software Engineering Institute. Fowler works with Pentagon officials, cyber intelligence officers, and the private sector to identify key cyber assets, secure them from cyberattacks, and coordinate a response should hackers infiltrate secured systems. "Ultimately, it absolutely could happen," Fowler said. "Yeah, that thought keeps me up at night, in terms of what portion of our critical infrastructure could be really brought to its knees."

The *Tribune Review* reports that the United States, along with most industrialized countries work diligently to build, arm, and aim cyberattacks that can be initiated at the first provocation of war. Until then, militaries and intelligence agencies conduct cyber espionage, often to send a message or disrupt an adversary's capabilities.

For example, the United States and Israel launched the Stuxnet attack on Iran's uranium-enrichment facilities in 2010. The FBI has also discovered hackers tied to the Iranian government breaking into the systems of American defense contractors, universities, and energy companies. DHS has found Russian hackers placing destructive software into American power grid, telecommunications, and oil distribution systems. Security analysts at FireEye report that in the early stages of Russia's involvement in the Ukrainian conflict, malware was detected erupting from both countries.

Analysts have not detailed the specific intent of the potential cyberattacks, but they do suggest that "computer network operations are being used as one way to gain competitive advantage in the conflict."

Before countries consider going to war, they must lay the groundwork for cyberattacks, said Kenneth Geers, a former U.S. representative to NATO's cooperative cyber defense center in Estonia and cybersecurity expert who conducted the FireEye research.

"Because both weapons systems and critical infrastructure use computers and networks to run and operate, they are much more than legitimate targets," said Geers. "They are absolutely necessary to attack and undermine on a daily basis. … If things go bad, nobody is going to forgive you for not having done this already."

Some critics have questioned the likelihood of a cyber-9/11, noting that there has yet to be a major cyberattack aimed at critical infrastructures, despite an increase in sophisticated hackers. "I kind of hate to be that guy," said Dan Tentler, a cybersecurity tester based in San Diego. "But I have to ask: If these systems have been open and vulnerable for 15-plus years, why haven't the bad guys done bad stuff yet?" Tentler believes hackers have too much to lose to disrupt the same systems they use to steal information and money.

CERT's Fowler agrees. "There's no reason to drop a nuclear bomb if you can come in through a door or come in through a window," she said. "Right now, a lot of money is being made — and stolen — by these organizations. And we haven't seen the need for the big cyber 9/11 yet."

Nader Mehravari, a senior member of CERT's Cyber Risk Management Team, points out that "The risk is higher. Not only because there are more clever adversaries but because there are things that we have done to ourselves." Mehravari is referring to the decision by critical infrastructure companies to connect their systems online for off-site control and 24/7 monitoring.

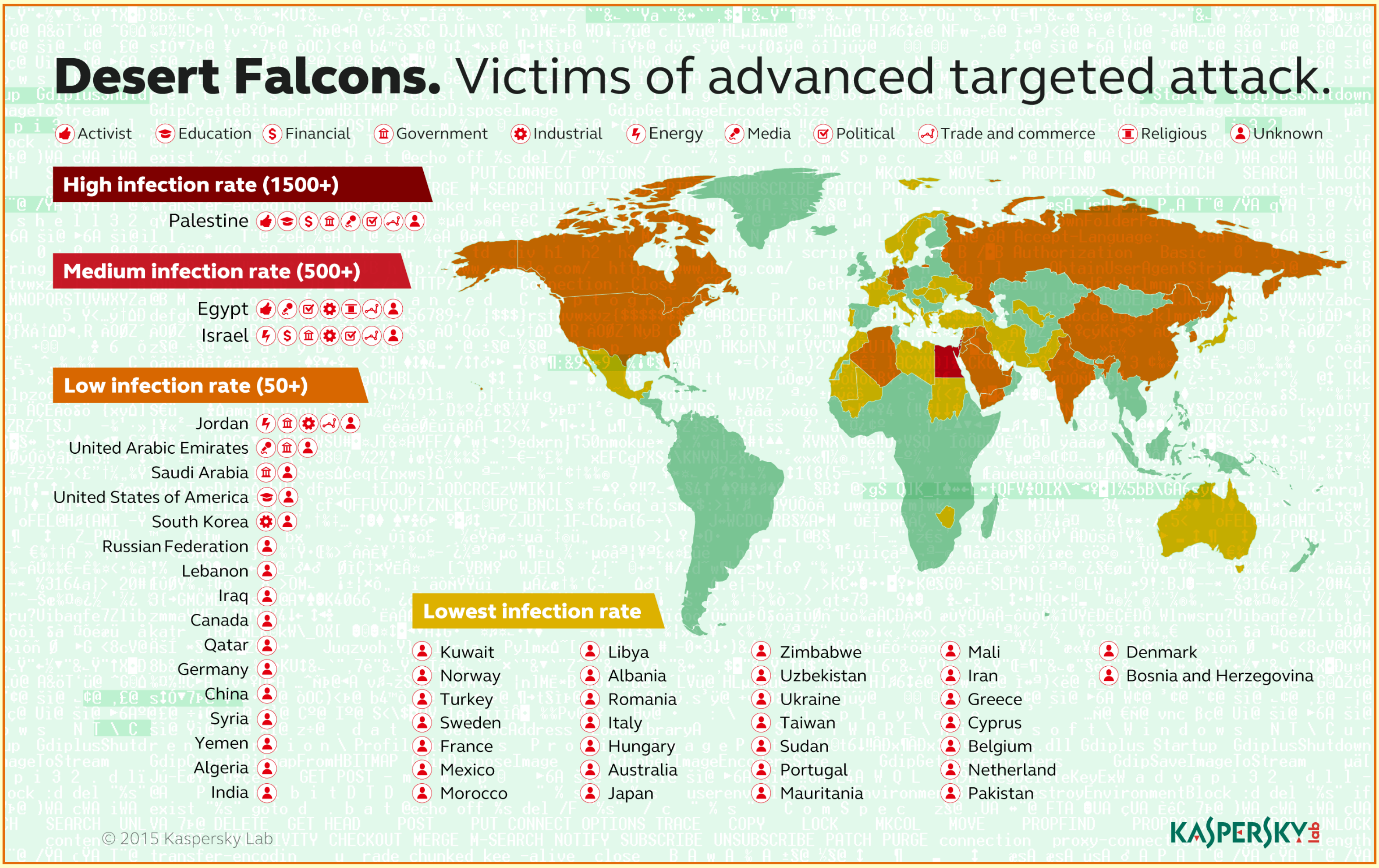
ProjectSHINE

Project SHINE, a private research project, found more than two million industrial control systems connected to the Internet. More than 30 percent of those systems are based in the

United States. "The people who conceived of this convenience did not take into account the evil that is out there," said Joji Montelibano, the technical manager of CERT's Vulnerability Analysis Team.

First known Arabic cyber-espionage group attacking thousands globally

Source: http://www.homelandsecuritynewswire.com/dr20150219-first-known-arabic-cyberespionage-group-attacking-thousands-globally-kaspersky-lab



Feb 19 – **The Kaspersky Lab Global Research and Analysis Team the other day announced the discovery of Desert Falcons, a cyber-espionage group targeting multiple high profile organizations and individuals from Middle Eastern countries. Kaspersky Lab said its experts consider this actor to be the first known Arabic group of cyber mercenaries to develop and run full-scale cyber-espionage operations.**

- The campaign has been active for at least two years. The Desert Falcons started developing and building their operation in 2011, with their main campaign and real infection beginning in 2013. The peak of their activity was registered at the beginning of 2015
- The vast majority of targets are based in Egypt, Palestine, Israel, and Jordan
- Apart from the Middle East countries focused on as initial targets, the Desert Falcons are also hunting out of the territory. In total, they have been able to attack more than 3,000 victims in 50+ countries globally, with over one million files stolen
- The attackers utilize proprietary malicious tools for

attacks on Windows PCs and Android-based devices

- Kaspersky Lab experts have multiple reasons to believe that the attackers behind the Desert Falcons are native Arabic speakers

The list of targeted victims include military and government organizations — particularly employees responsible for countering money laundering as well as health and the economy; leading media outlets; research and education institutions; energy and utilities providers; activists and political leaders; physical security companies; and other targets in possession of important geopolitical information. In total Kaspersky Lab experts were able to find signs of more than 3,000 victims in 50+ countries, with more than one million files stolen. **Although the main focus of Desert Falcons' activity appears to be in countries such as Egypt, Palestine, Israel, and Jordan, multiple victims were also found in Qatar, KSA, UAE, Algeria, Lebanon, Norway, Turkey, Sweden, France, the United States, Russia, and other countries.**

Deliver, infect, spy

The main method used by the Falcons to deliver the malicious payload is spear phishing via e-mails, social networking posts, and chat messages. Phishing messages contained malicious files (or a link to malicious files) masquerading as legitimate documents or applications.

Desert Falcons use several techniques to entice victims into running the malicious files. One of the most specific techniques is the so-called right-to-left extension override trick.

This method takes advantage of a special character in Unicode to reverse the order of characters in a file name, hiding the dangerous file extension in the middle of the file name and placing a harmless-looking fake file extension near the end of the file name.

Using this technique, malicious files (.exe, .scr) will look like a harmless document or pdf file; and even careful users with good technical knowledge could be tricked into running these files. For example, a file ending with .fdp.scr would appear .rcs.pdf.

After the successful infection of a victim, Desert Falcons would use one of two different Backdoors: the main Desert Falcons' Trojan or the DHS Backdoor, which both appear to have been developed from scratch and are in continuous development. Kaspersky Lab experts were able to identify a total of more than 100 malware samples used by the group in their attacks.

The malicious tools used have full Backdoor functionality, including the ability to take screenshots, log keystrokes, upload/download files, collect information about all Word and Excel files on a victim's Hard Disk or connected USB devices, steal passwords stored in the system registry (Internet Explorer and live Messenger) and make audio recordings.

Kaspersky Lab experts were also able to find traces of activity of a malware which appears to be an Android backdoor capable of stealing mobile calls and SMS logs.

Using these tools the Desert Falcons launched and managed at least three different malicious campaigns targeting different set of victims in different countries.

A pack of Falcons on the hunt for secrets

Kaspersky Lab researchers estimate that at least 30 people, in three teams, spread across different countries, are operating the Desert Falcons malware campaigns.

"The individuals behind this threat actor are highly determined, active and with good technical, political and cultural insight. Using only phishing emails, social engineering and homemade tools and backdoors, the Desert Falcons were able to infect hundreds of sensitive and important victims in the Middle East region through their computer systems or mobile devices, and exfiltrate sensitive data. We expect this operation to carry on developing more Trojans and using more advanced techniques. With enough funding, they might be able to acquire or develop exploits that would increase the efficiency of their attacks," said Dmitry Bestuzhev, security expert at Kaspersky Lab's Global Research and Analysis Team.

Kaspersky Lab says its products successfully detect and block the malware used by Desert Falcons threat actors.

— *Read more in "The Desert Falcons targeted attacks," Version 2.0,* Kaspersky's SecureList *(17 February 2015)*

HTTP/2

Source: https://http2.github.io/

HTTP/2 is a replacement for how HTTP is expressed "on the wire." It is **not** a ground-up rewrite of the protocol; HTTP methods, status codes and semantics are the same, and it should be possible to use the same APIs as HTTP/1.x (possibly with some small additions) to represent the protocol.

The focus of the protocol is on performance; specifically, end-user perceived latency, network and server resource usage. One major goal is to allow the use of a single connection from browsers to a Web site.

The basis of the work was SPDY, but HTTP/2 has evolved to take the community's input into account, incorporating several improvements in the process.

HTTP/2.0

There is emerging implementation experience and interest in a protocol that retains the semantics of HTTP without the legacy of HTTP/1.x message framing and syntax, which have been identified as hampering performance and encouraging misuse of the underlying transport.

The Working Group will produce a specification of a new expression of HTTP's current semantics in ordered, bi-directional streams. As with HTTP/1.x, the primary target transport is TCP, but it should be possible to use other transports.

Work will begin using draft-mbelshe-httpbis-spdy-00 as a starting point; proposals are to be expressed in terms of changes to that document. Note that consensus is required both for changes to the document and anything that remains in the document. In particular, because something is in the initial document does not imply that there is consensus around the feature or how it is specified. The deliverable of the WG is HTTP/2.0, and there is no consideration of preserving backwards compatibility with the initial starting point.

As part of the HTTP/2.0 work, the following issues are explicitly called out for consideration:

- A negotiation mechanism that is capable of not only choosing between HTTP/1.x and HTTP/2.x, but also for bindings of HTTP URLs to other transports (for example).
- Header compression (which may encompass header encoding or tokenisation)
- Server push (which may encompass pull or other techniques)

It is expected that HTTP/2.0 will:

- Substantially and measurably improve end-user perceived latency in most cases, over HTTP/1.1 using TCP.
- Address the "head of line blocking" problem in HTTP.
- Not require multiple connections to a server to enable parallelism, thus improving its use of TCP, especially regarding congestion control.
- Retain the semantics of HTTP/1.1, leveraging existing documentation (see above), including (but not limited to) HTTP methods, status codes, URIs, and where appropriate, header fields.
- Clearly define how HTTP/2.0 interacts with HTTP/1.x, especially in intermediaries (both 2->1 and 1->2).
- Clearly identify any new extensibility points and policy for their appropriate use.

The resulting specification(s) are expected to meet these goals for common existing deployments of HTTP; in particular, Web browsing (desktop and mobile), non-browsers ("HTTP APIs"), Web serving (at a variety of scales), and intermediation (by proxies, corporate firewalls, "reverse" proxies and Content Delivery Networks). Likewise, current and future semantic extensions to HTTP/1.x (e.g., headers, methods, status codes, cache directives) should be supported in the new protocol.

Note that this does not include uses of HTTP where non-specified behaviours are relied upon (e.g., connection state such as timeouts or client affinity, and "interception" proxies); these uses may or may not be enabled by the final product.

Explicitly out-of-scope items include:

- Specifying the use of alternate transport-layer protocols. Note that it is expected that the Working Group will work with the TLS working group to define how the protocol is used with the TLS Protocol; any revisions to RFC 2818 will be done in the TLS working group.
- Specifying how the HTTP protocol is to be used or presented in a specific use case (e.g., in Web browsers).

The Working Group will coordinate this item with:

- The TLS Working Group, regarding use of TLS.
- The Transport Area, regarding impact on and interaction with transport protocols.
- The HYBI Working Group, regarding the possible future extension of HTTP/2.0 to carry WebSockets semantics.

The Working Group will give priority to HTTP/1.1 work until that work is complete.

CoBRA's Damage Assessment Module

Source:http://www.cobra2020.com/Products/DamageAssessmentModule.aspx?utm_source=CoBRA+Software&utm_campaign=8c324b3c4c-1_26_2015+Dam+email+to+IAEM+2014&utm_medium=email&utm_term=0_31567c621a-8c324b3c4c-148518757

CoBRA's Damage Assessment Module (D.A.M.) is a new online tool available for local emergency managers, state recovery directors, and FEMA recovery experts. D.A.M. helps local emergency managers and state recovery personnel quickly gather Preliminary Damage Assessments for faster submission and accuracy of disaster damages.

D.A.M. tracks and records post event data; including the number of sites and facilities affected, total property value loss, location of the damage, and allows for unlimited file uploads including pictures, video, and digital documents.

By using D.A.M. local emergency managers:

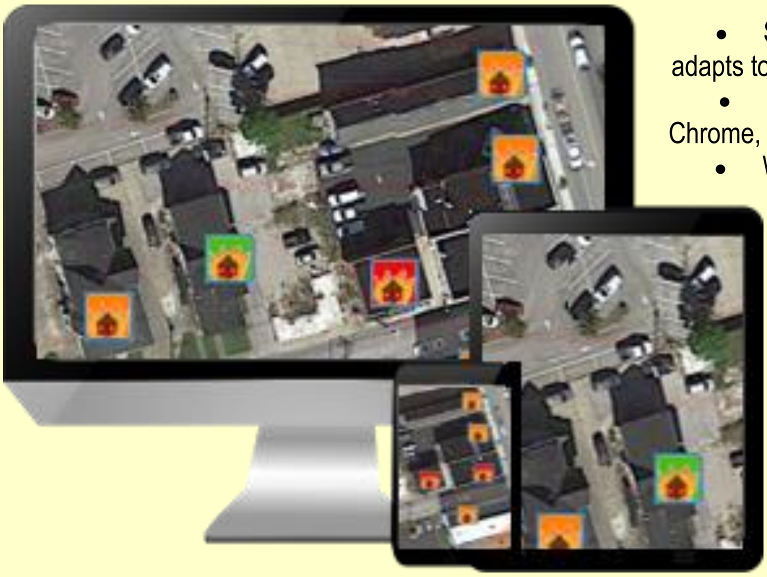
- Accurately justify their cost reimbursements
- Helps state recovery personnel speed up the Presidential Disaster Declaration for their state
- And help FEMA Recovery experts gather more accurate information faster resulting in the community recovering and rebuilding faster.

CoBRA's D.A.M. is hosted on Amazon AWS servers with a 99% up time guarantee. By accessing D.A.M. through a dedicated website your agency gets access to a robust damage assessment tracking program with ZERO server costs to your agency.

FAST DAMAGE ASSESSMENT REPORTS

- Quickly capture the Who, What, When, Where, and How Much of disaster damages in real time
- Add unlimited number of photos, video, and files to each record
- Simplified submission of damage reports to requesting agencies
- Export to CSV files and Google Earth for rapid sharing
- Batch print all reports to PDF

MULTI-DEVICE FRIENDLY



- Smart interface automatically adapts to your device screen
- Runs on Firefox, Google Chrome, and Internet Explorer browsers
- Wearable, smartphone, tablet, Mobile Data Terminal and multi screen
- Upload pictures from devices camera
- Use devicesGPS

CONNECTIVITY NOT REQUIRED

- Desktop and laptop application available even when Internet connectivity is lost
- Automatically syncs with the server when Internet connectivity is restored
- Unlimited number of desktop and laptop programs permitted
- Updates with server automatically

INSTANT AFFORDABLE SOLUTION

- Host in your own IT server farm or
- Use our Amazon AWS backed hosted service
- Flexible pricing for every budget

MAPPING

- Real time, collaborative mapping across all platforms
- Automatically geo-tag all damage reports in real time
- Available satellite imagery and street maps
- Integrates with other mapping and GIS applications
- Draw sketches and annotate map with points, lines and polygons
- Export data to Google Earth for information sharing with other EOC's

W Columbia St

INTEGRATES WITH OTHER SYSTEMS

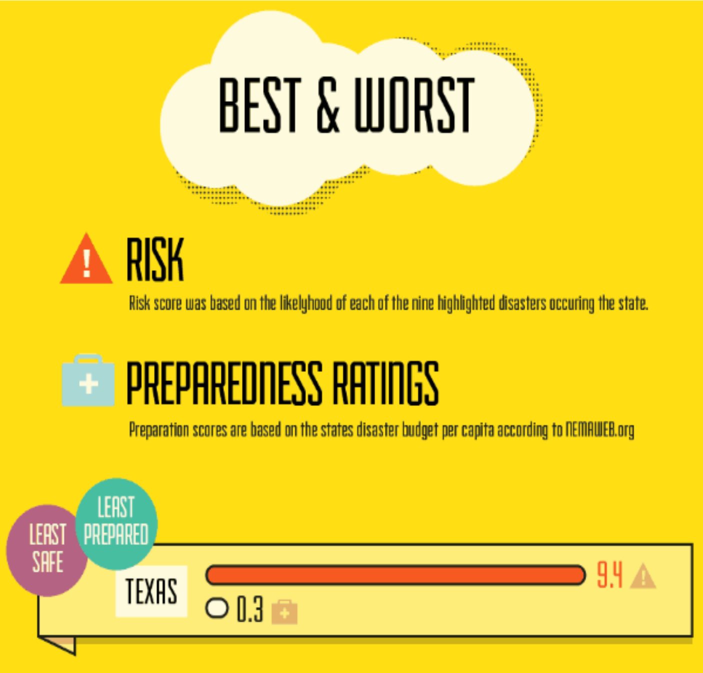
- Open API and free Software Developer Kit allows information sharing with other systems
- Connects with other Emergency Management Information Systems used by different jurisdictions
- Works with and can enhance your current legacy systems

ATTACH PHOTOS, VIDEOS, AND DOCUMENTS

- Attach photos, videos, and documents to every record
- Unlimited number of photos and videos allowed
- All photos and videos geotagged and displayed on map
- Hover over record for quick glance of photos
- Create a post incident record for reporting and lessons learned

USA: Is Your State Prepared for a Natural Disaster? Check Out These Rankings and See Where You Stand

Source: http://www.theblaze.com/stories/2014/12/08/is-your-state-prepared-for-a-natural-disaster-check-out-these-rankings-and-see-where-you-stand/



In an infographic posted earlier this year, Foodstorage.com's "Prepper Feed" blog came up with a measure of each state's disaster-preparedness by analyzing the risks each state faces from different natural calamities and stacking that against each state's per-capita disaster budget.

As you might expect, those criteria led to a ranking system that favors lower-population, bigger-government states.

The worst-prepared state, according to the rankings: Texas, which faces threats from hurricanes, flooding and tornadoes but which has a fairly low per-capita disaster budget for its 26.5 million people.

Meanwhile, states with smaller populations fared much better: Wyoming, North Dakota and Delaware nabbed the top three spots.

3-D Laser Scanner Could Revolutionize Police, Security Procedures

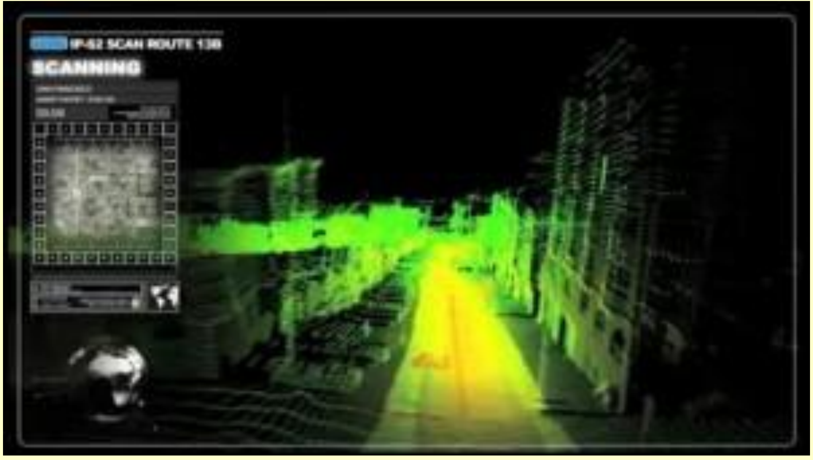
Source: http://pittsburgh.cbslocal.com/2015/01/27/3-d-laser-scanner-could-revolutionize-police-security-procedures/

It's something straight out of the TV show CSI. And it's being used by emergency agencies all over the country.

Over the past couple days, Pittsburgh emergency management and homeland security have been training to use the 3-D laser scanner.

Nina DiCarlo East is the manager of the company bringing the device here.

“The way emergency management departments and homeland security plan to use them is with their critical infrastructure in the City of Pittsburgh, doing the different fields and stadiums, convention center as well as with the police departments,” said East.



In layman terms, this is how the 3D laser scanner will work. It will allow emergency teams to know every nook and cranny in any building that has been scanned.

And there is more – how many times have you been behind an accident, stuck in traffic for hours as police reconstructed the seen and do measurements? The 3-D scanner will change all of that.

“You won’t have a police officer measuring everything by hand,” said East. “He’s able to actually have it measured automatically b the 3-D laser scan. So you will be taking a four-hour police scene to an hour, so the road is open faster.”

The 3-D scanner will also prove beneficial in court during jury trials.

“Instead of taking them to the crime scene, you can bring the crime scene to the jury in the courtroom in 3-D,” said East. “Actually see it in person and not have to imagine what someone is telling them. They see it firsthand.”

The $100,000 use to buy two scanners came from homeland security funds and they are already being used. PNC Park was the first of several facilities where large crowds gathered to be scanned.

So where will all of the information be stored?

Raymond DeMichiei, Deputy Dir. Of Emergency Management and Homeland Security says, “on thumb drives, on DVD, in all likelihood will be stored at the site.”

Representatives learning the system are from various counties making up the Region 13 task force.

How Robots Are Changing Disaster Response and Recovery

By Elaine Pittman

Source: http://www.emergencymgmt.com/disaster/How-Robots-Are-Changing-Disaster-Response-Recovery.html

Robin Murphy is a leader in the field of disaster robotics, having started working on the topic in 1995 and researching how the mobile technologies have been used in 46 emergency responses worldwide. She has developed robots that have helped during responses to numerous emergencies, including 9/11 and Hurricane Katrina. As director of the Center for Robot-Assisted Search and Rescue at Texas A&M University, Murphy works to advance the technology while also traveling to disasters when called upon to help agencies determine how robots can aid the response. The center's first deployment was in response to 9/11, which also was the first reported use of a robot during emergency response.

Emergency Management: Since 9/11, how have you seen the use of robots in disasters change?

Robin Murphy: We started out in 2001 and up until 2005 you didn't see the use of anything but ground robots. Everything was very ground-centric, and I think that reflected the state of the technology. For years we had bomb squad robots, which were being made smaller and smaller for military tactical operations so that gave them a tool that was pretty easy to use. Starting in 2005, we saw the first use of small unmanned aerial vehicles that were being developed primarily for the military market and those were very useful. Those have really come up and, in fact, since 2011, I've only found one disaster that didn't use an unmanned aerial vehicle and that was the South Korea ferry where they used an underwater vehicle. So we went from ground robots dominating to about 2005 and then we started shifting toward unmanned aerial vehicles. In about 2007, it became much more commonplace to see underwater vehicles being used. Then starting in about 2011, I think if you have a disaster and you're an agency and you haven't figured out a way to use a small unmanned aerial system, it's kind of surprising.

EM: Is one of the issues that people are waiting for FAA regulations to use UAVs?

RM: Every single disaster since about 2011, but definitely since 2012, looking at the 46 disasters we've kept tabs on, have used unmanned aerial systems, including the ones here in the United States. I would not say the adoption problem is the FAA regulations. It takes very little time to get an emergency COA [certificate of authorization]. It does take time to get some of the paperwork in advance done to fly a regular COA but the FAA has given jurisdictional COAs. The emergency COAs take a very short period of time — it's knowing the paperwork, like with any new technology.

The deterrent to adoption seems to have been the lack of money to flat out purchase them. They're basically computers and you know how fast the technology for your cellphone and computer changes, you wouldn't expect to have a computer that's 10 years old, so you wouldn't buy these the way you buy big equipment. We're suggesting that agencies look at plans that allow them to lease the technology. And also because it's a new technology, you don't know what that means in terms of training and how it's going to be integrated and that means they don't have to recoup some of the training and maintenance costs right off the bat.

EM: What are you currently working on?

RM: I work mostly on the human factor side: How people actually use these. I am not worried about whether a UAV is going to fall out of the sky or a ground robot's wheels will stop turning. In my book, *Disaster Robotics*, I go back over 34 disasters, of which I was in a bunch. If you look at the data that's available, there were 13 terminal failures where the robots failed for some reason and that caused the mission to be aborted.

In about 51 percent of the cases it was human error. When I go back and analyze that I see that it's human error, but it was the designer — the designer didn't give it an interface that allowed the user to have the right type of information to make a different or better decision. You can only see what you can see.

We're also very interested in how these technologies change the way emergency response works. What we saw at the Washington state mudslide was that everybody's thinking "these UAVs will be useful for ESF [emergency support function] 9 for urban search and rescue" but actually they're more useful in that particular case, in a mudslide, for public safety and you can start thinking about ESF 14 and recovery. [Questions include:] How are you going to share that information? How are you going to do that without creating a data avalanche that just overwhelms different decision-makers who need to share, to plan, to interact with each other? And if I want to use this robot and you want to use it and we both want to point it in different directions, how do we handle that? So how do you get these interfaces that let people interact in real time and then process the data and share and work together?

We've got a group of students that have put together what we call the Skywriter interface that lets somebody with a tablet, laptop or mobile phone see what a UAV or robot is seeing and communicate to the operator or system what they want to do, like circle or draw an arrow, which indicates where to go, or follow my finger and track this.

EM: When you deploy to a disaster, what's your role there?

RM: We're always invited in, we do not self-deploy. Our center, this is something frankly that I am little disappointed that we're still doing, I had hoped that at this point everybody would have robots, but we can provide robots. We can usually provide robots through our Roboticists Without Borders program where members train with us beforehand and then when we're called out, they will donate their equipment and time. So we go out and our role is to first off see, what's the right technology for what they're trying to do? There are some times when a robot isn't going to work because you can't afford in a disaster to make anything worse, so we have to be conservative. We act as a dating service. What we've found is that most responders prefer to work with us side by side. We'll drive and you tell us what to do. We also do formal studies and what we've found is that in looking at the video data and the sensor data coming from robots, two heads are nine times better than one head. Having a team work together really takes off the cognitive load, one person will catch something that the other person didn't and it just adds a vast improvement to performance. … With that said, I would love to be out of business, I would be just as happy for groups to have robots on their own. I would like the data though; I love learning from the practitioners what's working and what's not.

EM: Have you been working on anything in response to public health needs like for the Ebola response?

RM: We find that in Ebola a lot of people are thinking about clinical applications, like replacing the nurse. Nurses and doctors are hard to replace and duplicate; robots rarely are cost-effective at replacing what humans do. They're often better at giving some capability that you didn't have before. So in this case, rather than looking at clinical needs, we've looked at logistical needs and the fact that a lot of people involved in health aren't really doing health work, they're cleaning up messes, they're hauling all of these sheets that are contaminated, they're trying to move people around. So having one person instead of four doing that begins to be more of what the military calls a "force multiplier" and becomes much more efficient. There are things like that that exist. There's general reconnaissance: How long is the line outside? What's going on in the villages in the rainforest, do they seem empty? Is there dirt overturned that may indicate graves? That can indicate what's going on.

We're also looking at clinical but that's going to be much more specialized. We like to work with the practitioners and find out what's going to be the most bang for the buck. If there's one thing to do to make your life easier, what would that be?

EM: Looking to the future, where do you see disaster robotics headed in the next five to 10 years?

RM: There's that idea of adoption, which will hopefully continue to accelerate.

In the future, for the new technology, I expect to see three things: Better software on what we call emergency informatics; it's how you share the data and how you visualize it. In ground robots, I am so excited at work at looking at burrowing robots. The big value in most big building collapses lies in the smaller the better, what do you do when there's not an obvious void and can you get something to literally snake and nudge and worm its way through there. There are some animals that do that — there's a sand lizard and types of snakes that navigate in the ground — so we're doing some work with Georgia Tech and Carnegie Mellon on that. There are also some great advances being made in manipulation. Initially I would characterize the first decade of robots as having been all about allowing the responders to see at a distance, but now we're seeing a shift. We can see at a distance but now we would like to poke things, we would like to move them over, we would like to drop off things. So we need to act at a distance and not just see at a distance. There's some advances in robot manipulation that are coming up and are very exciting and we'll be incorporating those into future work.

***Elaine Pittman** is the associate editor of* Emergency Management *magazine. She covers topics including public safety, homeland security and lessons learned. Pittman is also the associate editor for* Government Technology *magazine.*

Should Background Checks be Required for Emergency Volunteers?

Source: http://www.emergencymgmt.com/disaster/Should-Background-Checks-Required-Emergency-Volunteers.html

When disaster strikes in Palm Beach County, Fla., a team of volunteers trained by county emergency managers can be deployed as the first line of defense, helping their communities with everything from search and rescue to basic first aid to putting out small fires.

They can also be called upon to distribute or install smoke alarms, hand out disaster education materials or replace smoke alarm batteries in the homes of the elderly, according to a brochure about the program.

But there's no requirement that they be subject to any kind of criminal background check.

That could change after a concerned Boynton Beach resident complained to the Florida Division of Emergency Management's Inspector General. In a report released last week, the inspector recommended that background checks be a condition of the grants doled out for the program.

To get an ID badge, helmet, vest and other equipment that designates them as part of the Community Emergency Response Team, residents must fill out paperwork and attend hours of training.

The lack of background checks, though, could **"create the opportunity for felons to use these credentials to gain access to some of Florida's most vulnerable population: the disabled, the elderly and disaster survivors,"** the report concluded.

Jody Gorran, who brought his concerns to the inspector general's office in August after going through the program and discovering background checks weren't mandated, said that's exactly what he was worried about. It is "outrageous" that Community Emergency Response Team volunteers aren't properly vetted, he said.

"You get access to peoples' homes," said Gorran, 64, a retired business owner and volunteer firefighter. "You get access to situations where you have this trust placed upon you that possibly you don't deserve. I'd much rather not have seen anybody trained than see anybody trained who might have a criminal record — who might do something to somebody."

The program got its start in Los Angeles in 1986, born out of the deaths a year earlier of 100 untrained volunteers who sprang into action after an 8.1-magnitude earthquake devastated Mexico City.

From that disaster, Los Angeles fire department personnel saw a need to train volunteers to help themselves and others, and launched a Community Emergency Response Team. In the early 1990s, officials with the Federal Emergency Management Agency decided to roll out the program nationwide.

It's now offered by more than 1,000 municipalities in 28 states and Puerto Rico, according to federal emergency officials.

There are programs across Florida in municipalities ranging from the town to county level. In South Florida, they include Fort Lauderdale, Pompano Beach, Margate, Davie, Coconut Creek, Jupiter, Weston, Sunrise and Delray Beach.

Funding is provided through the federal agency, which distributes it to the state level. The Florida Division of Emergency Management makes that money available to communities through grants. In fiscal year 2013-14, $290,000 was designated for Community Emergency Response Team training across the state, according to state-level emergency management officials.

The program is open to all residents – including, in some communities, high school students. Those who sign up learn how to help their community if a natural disaster or act of terrorism happens.

Over more than 20 hours of instruction and exercises, they are trained to perform activities including providing CPR, telling officials what kind of aid is needed, assisting in damage assessment, evacuation and sheltering and recognizing the signs of psychological trauma in the aftermath of a disaster.

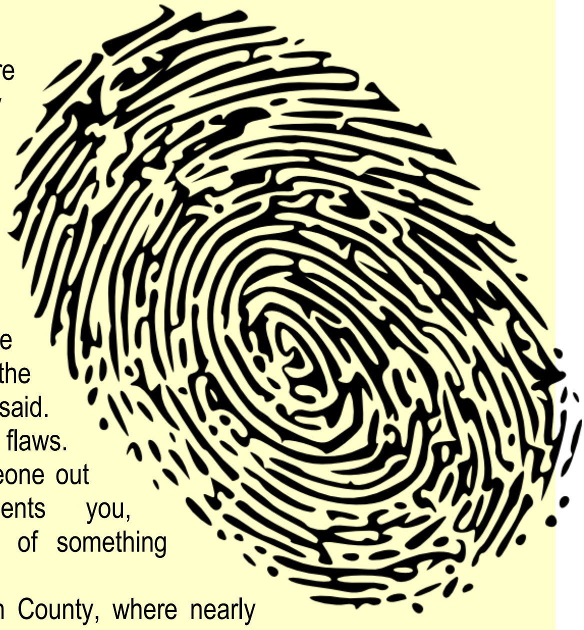
The concept is primarily aimed at neighbors helping neighbors. For that reason, Palm Beach County Administrator Robert Weisman said he thinks it's "a big step to start talking about doing background checks on these people in this program."

He said there are some things that occur at the community level that are outside the realm of government regulation.

"It's kind of like if you have that concern, maybe the program shouldn't exist at all," Weisman said.

Running background checks on volunteers would take away from the money available to train them, he said. He said he's also concerned about invading volunteers' privacy, and believes people may not want their neighbors to know about their pasts.

And even if background checks were mandated, Weisman said, they would only catch people who have been convicted of crimes, while other people could slip through.



"I believe there is a risk any time you have people doing anything, including our employees, that someone could violate the law," he said. "People have flaws. Any time someone out there represents you, there's a risk of something going wrong."

In Palm Beach County, where nearly 4,000 people have completed the Community Emergency Response Team training, commissioners might choose to discuss the recommendations in the report, Weisman said.

In March, the county received $8,402.50 from the Florida Division of Emergency Management for conducting a year's worth of basic training.

But it might not be left to the county to decide. The inspector general's recommendation was aimed at the Florida Division of Emergency Management. Officials there are reviewing the suggestion and safety is their first priority, said Aaron Gallaher, a spokesman for the division.

Whether or not to do background checks is currently left to the discretion of each community that receives the funding. Some require them; others don't.

Gallaher said the Florida Division of Emergency Management is not aware of any cases in which a felon joined a Community Emergency Response Team or a resident's safety was put at risk by a volunteer.

But Gorran said that's beside the point. He said community members who see the badge, helmet and other gear given to Community Emergency Response Team members see them as "the good guys" and don't realize they haven't been thoroughly screened.

And he's not done yet.

No stranger to tackling what he perceives as threats to public safety, Gorran worked on the federal Volunteers for Children Act signed into law in 1998, which allows nonprofits that serve children the right to get national fingerprint checks on volunteers.

Now that the inspector general has agreed background checks should be done on response team volunteers, Gorran has been busy notifying community associations of the issue and trying to convince the county to review its trained volunteers. He said he plans to press for the change to be made nationwide. "I got exactly what I wanted," Gorran said, "and now I'm going to take it on the road."

EDITOR'S COMMENT: Excellent idea! The most important player in all state response plans should stop being in the corner and actively participate in the implementation of plans for a variety of disasters.

First responseFaster first aid for catastrophe victims

Source: http://www.homelandsecuritynewswire.com/dr20150204-faster-first-aid-for-catastrophe-victims

In mass casualty incidents, triage of the victims must be performed as quickly as possible, in order to evacuate and take them to appropriate hospitals. Today, first responders use colored paper tags to classify victims. In cooperation with an international group of partners, Fraunhofer FIT has developed an electronic gadget that may replace the colored paper tags in a triage. Beyond just visually tagging a victim, the device transmits, in real time, the victim's location and vital data, for example, heart rate, respiratory rate, and oxygen saturation, to emergency response control centers.

The first responders attach a color-coded plastic wristband (photo above) to each victim. Depending on their color, the wristbands incorporate different sets of technology, for example, a GPS module, an RFID chip and a wireless network module that communicates with the emergency response control center. An unharmed or slightly injured person will receive a wristband that includes only the GPS and the network module. Victims severely injured or in a critical state will receive wristbands with additional sensors that continually capture vital data and transmit them to the control center. A Fraunhofer release notes that each wristband also functions as a node in a wireless network. Even if the regular mobile phone networks are down, our system is still operational. It sets up an ad-hoc ZigBee network, a low-bandwidth wireless network that combines long range and low energy consumption. The wristbands have the necessary technology built in. First responders get equipped with Triage Relays that cache, backup and retransmit the data.

"The real-time data from the triage wristbands can be displayed on the large screens in the emergency response control center, but also on the tablets or smartphones of medical staff in the field. First responders and response coordinators thus have a precise picture of the situation on the ground. Rescuers see at a glance where the majority of severely injured casualties are located and can direct the rescue activities accordingly," explains Dr. René Reiners, project manager at Fraunhofer FIT. The **system was developed in the European BRIDGE project where FIT's User-Centered Computing department (headed by Dr. Markus Eisenhauer) is the technical coordinator.**

FIT will also demonstrate a pair of smartphone apps that lets victims communicate with first responders even if the mobile phone networks are down. One component of the solution is an app on the victim's smartphone. When the user activates it, it sets up a Wi-Fi access point and sends an emergency message, for example, "Buried Alive," instead of the phone's regular Wi-Fi Service Identifier (SSID). The app on the first responder's phone scans for WLAN networks in its vicinity detects the emergency message and sends a response signal to the victim's app. The solution we demonstrate uses stock Android smartphones that give it a range of up to 100 meters.

Disaster response Before-and-after aerial imagery of infrastructure to help first responders

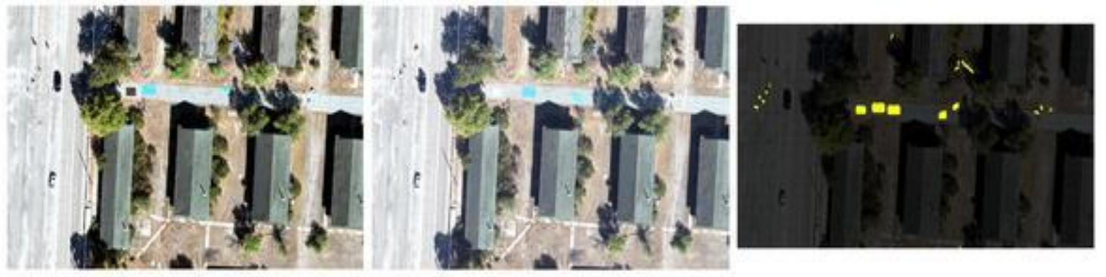
Source: http://www.homelandsecuritynewswire.com/dr20150206-beforeandafter-aerial-imagery-of-infrastructure-to-help-first-responders

When disaster strikes, it is important for responders and emergency officials to know what critical infrastructure has been damaged so they can direct supplies and resources accordingly.

Doug Stow, a geography professor from San Diego State University, is developing a program that uses before-and-after aerial imagery to reveal infrastructure damage in a matter of minutes.

"After a disaster, emergency responders need to know what's damaged and what's functioning," said Stow, who recently received $365,000 from the National Science Foundation to support this research.

A SDSU release reports that the work builds on ongoing research by Stow and Pete Coulter of the university's Center for Earth Systems Analysis Research for the U.S. Department of Homeland Security and the Navy Postgraduate School.



There are subtle differences between the first two images, captured by the computer program pictured in the right-most image (➤ yellow markings). Photos: Doug Stow and Pete Coulter.

Bird's-eye patrol

The idea behind the project is this: Emergency officials identify ahead of time the critical infrastructure they will need in case of an emergency — power stations, bridges, dams, hospitals, and others — and researchers like Stow send out unmanned aerial vehicles (UAVs) and piloted light sport aircraft (LSA) to take bird's-eye pictures of the intact buildings and environment.

During the flight, the UAVs record their GPS locations and altitude and report back with both their positions and the images, which are filed into a computer program. If a disaster occurs, emergency managers can immediately send back a UAV or LSA to take an aerial image from the exact same location and altitude, process the before-and-after images to detect changes, and report back with a damage map.

A computer program compares the two images and does a highly advanced version of a "spot-the-differences" game, pointing out to researchers and officials where the images differ. These differences can highlight walls that have crumbled, ceilings that have collapsed, roads that have buckled, and other signs of infrastructure damage.

Several other SDSU researchers, students and graduates are also supporting the project. Electrical engineer Sunil Kumar is helping to determine how to optimize the wireless image and map transfer between ground control and the aircraft.

Geography graduate students Andrew Kerr and Manny Storey are involved in the project, and Christopher Lippitt, a graduate of the SDSU-University of California, Santa Barbara, joint doctoral program is the institutional principal investigator for the University of New Mexico, which is collaborating with SDSU on the project.

Accounting for shadows

The key to all of this is being able to take clear photos from exactly the same place and angle, almost as if a camera was mounted in the sky, Stow said.

"The goal is for these images to look like they were taken by a stationary security camera, even though they were taken by an aircraft hundreds of feet overhead," he said.

If all goes well and aircraft can be deployed quickly, Stow added, that information can be available to emergency responders within an hour or two after a disaster.

The tricky part from a computational perspective, he said, is accounting for ordinary changes that occur in a picture, such as the position of shadows or the location of cars in a parking lot. That's a challenge Stow and his colleagues are currently working on.

In the meantime, the researchers are working with San Diego County's Office of Emergency Services, and its counterpart in Albuquerque, New Mexico, to run trials on simulated emergencies in order to optimize their software. Stow and Coulter are also developing a business, Repeat Station Imaging, through SDSU's Zahn Innovation Center, which will seek commercial applications for their imaging technology.

"We think the UAV imaging market is about to explode," Stow said. "Our technology can play an important role in its future."

A first: Engineering students design firefighting humanoid robot

Source: http://www.homelandsecuritynewswire.com/dr20150206-a-first-engineering-students-design-firefighting-humanoid-robot

Feb 06 – In fall 2014 in Mobile Bay, Alabama, **Virginia Tech engineering students made history during a five-minute demo that placed an adult-sized humanoid robot with a hose in front of a live fire aboard a U.S. Navy ship.**

The robot located the fire and sprayed water from the hose. Water blasted the flames.

The demo, four years in the making, is part of a new effort by the U.S. Navy better to assist sailors in fighting fires, controlling damage, and carrying out inspections aboard ships via user-controlled unmanned craft or humanoid robots. The **firefighting robot is named SAFFiR**, short for

Shipboard Autonomous Firefighting Robot, and the U.S. Office of Naval Research envisions a future — long off, but tangible — in which every ship has a robot as a tool for firefighters.

“It’s not going to replace Navy firefighters, it’s going to assist Navy firefighters,” said Viktor Orekhov of Morristown, Tennessee, who graduated in December 2014 with a doctorate in mechanical engineering.

A Virginia Tech release reports that Orekhov is one of fifteen engineering students in the Terrestrial Robotics Engineering and Controls Lab (TREC) and the Extreme Environments, Robotics & Materials Laboratory (ExtReMe) who helped conceive, design, build, and test SAFFiR.

SAFFiR is a bipedal 140-pound, 5-foot 10-inch humanoid robot that can walk, stretch and bend its legs, swivel its head, and hold and operate a hose with its hands. It has 33 degrees of freedom in movement. It can see in three formats: a standard stereo camera rig, lasers to provide precise ranges to obstacles, and stereo thermal imaging for range finding through smoke and detecting heat.

During a three-day demo in November 2014, students from the TREC and ExtReMe labs, along with faculty advisor Brian Lattimer, an associate professor with the Department of Mechanical Engineering, prepped SAFFiR for a fire suppression test onboard the former USS Shadwell, a decommissioned ship in Mobile, Alabama, now used as a damage control research center to test new shipboard firefighting techniques.

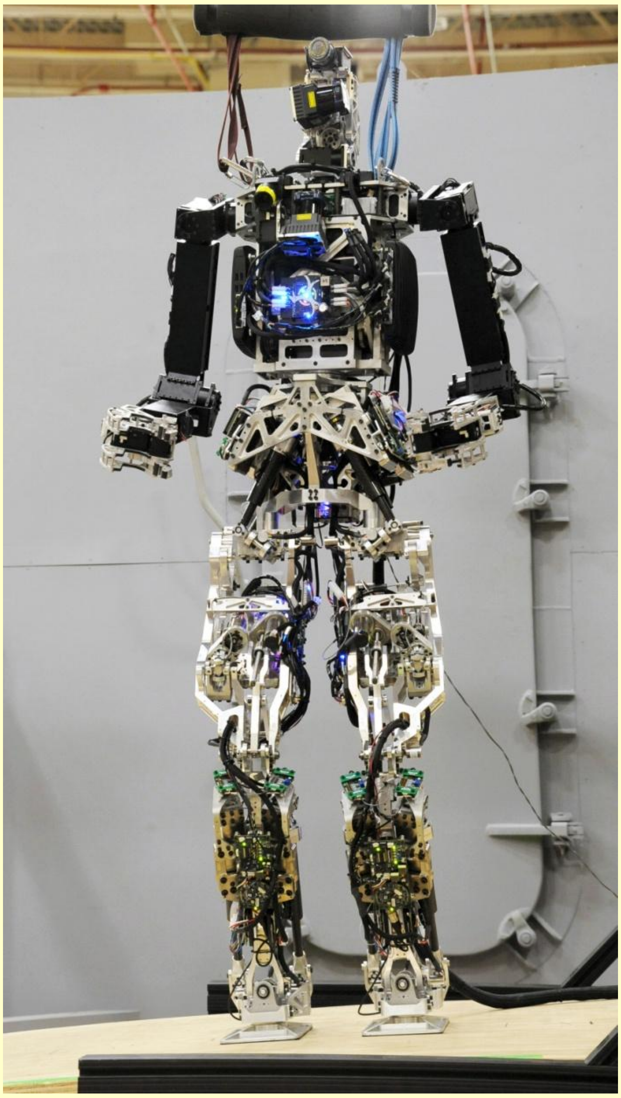
Along a slim, low-hung hallway, SAFFiR was tasked — programmed by the two labs’ imaging and manipulation team — to walk toward a sailor, stop, turn, locate the heat source of a fire behind a door, and (once the door opened) take a hose and blast the flames with water, all without falling or stopping.

The robot passed the test to the cheers of students and Navy personnel. “And that is that. Nicely done,” John Seminatore of Irvington, New York, a master’s student in mechanical engineering, said at the demo’s conclusion.

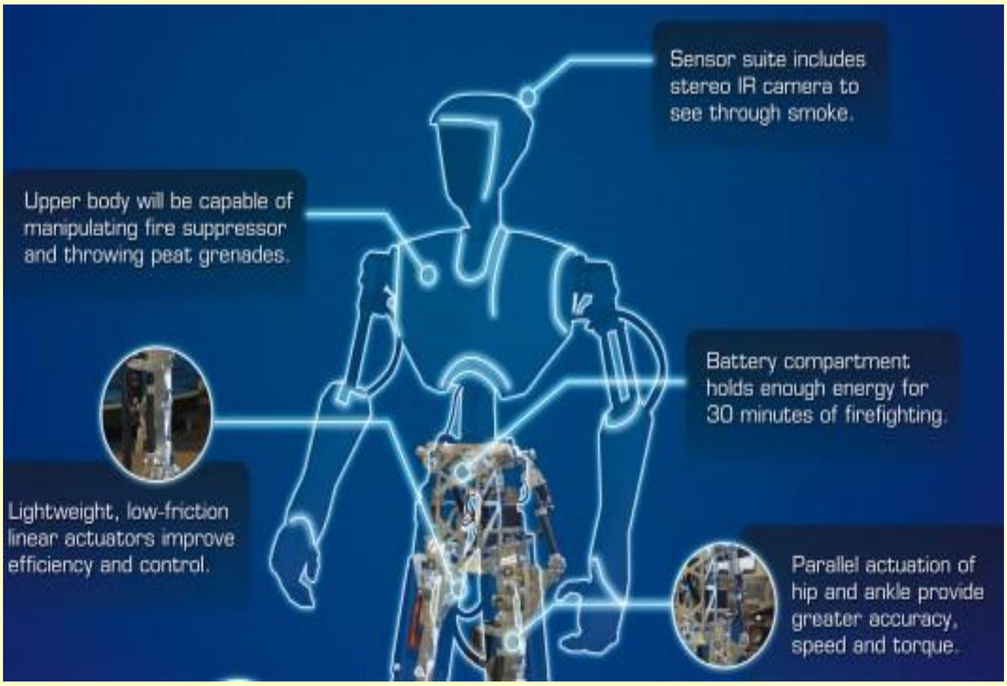
The release notes that students spent many hours aboard the ship prepping for the demo and hundreds of hours before that in their Goodwin Hall lab designing, fabricating, and testing SAFFiR. Unlike movies with CGI gimmickry to make robots appear to move, getting a real robot to walk upright is a challenge.

The Shadwell created extra obstacles: Heat from previous test fires has buckled its floors. In the hallway where SAFFiR walked, the floor slanted away from the path the robot has to take.

SAFFiR is, of course, a prototype, and the day of robot firefighters is long off. It is user-operated now, but long-range plans are for the robot to operate autonomously. Even with added intelligence to SAFFiR, it will take remote instruction from sailors and firefighters with safety as key.



“These robots can work closely with human firefighters without firefighters being directly exposed to steam or heat, fire and smoke,” Thomas McKenna, a program manager with the Office of Naval Research, said at the demo. Robots may one day patrol ships, he said, scanning for unnatural heat, smoke, or other issues and providing a “constant watch” against onboard dangers not detected by sailors.


Sensor suite includes stereo IR camera to see through smoke.
Upper body will be capable of manipulating fire suppressor and throwing peat grenades.
Battery compartment holds enough energy for 30 minutes of firefighting.
Lightweight, low-friction linear actuators improve efficiency and control.
Parallel actuation of hip and ankle provide greater accuracy, speed and torque.

The robot’s presence will be welcome. “Have you ever been on a ship that’s on fire? It’s terrifying,” said Dominique Pineiro, a Navy veteran on the Shadwell during the demo.

“That’s a fact.”

SAFFiR team members and the Navy unveiled the robot on 4 February, to media and the public at the Naval Future Force Science & Technology EXPO in Washington, D.C.

Future incarnations of SAFFiR already are planned with the Navy, according to Lattimer, with upgrades including improved movement. Funding from the Navy stands at $4.5 million and could increase as the project continues.

Days before the Expo, Seminatore — the SAFFiR student project manager at TREC — looked back on the demo of SAFFiR with relief and pride.

“We have demonstrated a real world application for humanoid robots that no one has done before,” said Seminatore, an Air Force veteran. “Manipulating an empty hose or walking down a hallway is very different than operating in a heat-warped soot filled corridor dragging a hose filled with water. It was a tense month leading up to the demo, we had never seen where we were testing, never used a real hose, never actually sprayed water. … The team did great and the robot performed like a champ.”

Executive Master of Professional Studies in Emergency and Disaster Management

Source: http://scs.georgetown.edu/departments/36/emergency-and-disaster-management/?&utm_source=EM_Weekly_News&utm_medium=Newsletter_Text&utm_campaign=FY15_PG_EDM_Newsletter_Text_EM_Weekly_News

GEORGETOWN UNIVERSITY
School of Continuing Studies
EXECUTIVE MASTER'S DEGREE
Emergency & Disaster Management

Expertly assist communities to become stronger and more resilient in the face of man-made and natural disasters. Through the Executive Master of Professional Studies in Emergency and Disaster Management program at Georgetown University, you can do just that by gaining the strategic and critical thinking skills you will need as a leader in the rapidly evolving profession of emergency management.

In this year-long cohort program, students will learn from emergency management experts with real world experience. Intensive field study introduces students to new challenges and new capabilities in the field. Sophisticated disaster simulations challenge students to apply real-time critical analysis to lifelike disaster scenarios and simulations.

Once you've completed the program's experiential journey through five graduate-level learning modules, **you will have the critical thinking and leadership skills to:**

- Respond to a range of uncertain, always-evolving disaster management complexities.
- Anticipate needs, evaluate alternative approaches and make critical decisions that facilitate "whole community" disaster response and disaster recovery operations.
- Work within the boundaries of emergency management ethics, laws and regulations.

A Unique Combination of Online and Field Study Learning Opportunities

Experience with natural and man-made disasters is the most meaningful teacher of effective emergency management practices. That's why onsite field study is part of the program's unique blend of online and onsite instruction.

Your emergency and disaster management studies will take you to four different locations for five unique onsite experiences:

- **Washington, D.C.**: Learn from the nation's experts about emergency management practices, laws, regulations and policies. Build the connections you need to advance as a leader in the emergency management profession. The Nation's Capital will be the site of the first module's introductory field study as well as the location of the Capstone's meta-scenario exercises – a true test of your emergency management skills under fire.
- **New Orleans**: Put yourself in the eye of Hurricane Katrina to fully understand the magnitude and scope of challenges faced by local, state and national emergency management communities in the face of severe natural disasters. Learn to lead, communicate and cope with the unexpected.
- **San Francisco Bay Area**: Visit the Lawrence Livermore National Laboratory and learn how emerging technologies are utilized to detect and predict the effects of hazardous threats.
- **Doha, Qatar**: Gain insights about the international dimensions of emergency and disaster management, especially with respect to the loss of critical infrastructure and emergency services.

Who Should Apply?

Our intensive one-year cohort program is designed for:

- **Public administrators, urban planners and elected officials** who want to build more resilient communities and foster greater individual participation in emergency preparedness and disaster response.
- **Policy makers and program directors** who are interested in developing emergency management strategies and operational approaches for the future.
- **Military, veterans and armed forces personnel** who desire a more in-depth understanding of domestic disaster response.
- **Private-sector professionals** who are interested in continuity of operations, protecting employees and supporting disaster response operations.
- **Recent college graduates** who are seeking an exciting career in the rapidly growing emergency management industry.
- **First responders** who aspire to take on emergency and disaster management leadership roles.

The skills gained from this program prepare students for a broad range of emergency service occupations in the government, non-profit and corporate sectors, such as careers in Emergency Management, Risk Communication, Public Health and Safety, and Policy and Planning.

Georgetown University's School of Foreign Service in Doha, Qatar

Doha, the thriving and beautiful capital city of Qatar, is the home of Georgetown University's top-ranked School of Foreign Service in Qatar. It is also the site of Education City, part of the Qatar Foundation for Education, Science and Community Development. Education City is a leading research and educational facility for many of the world's top universities, including Georgetown, Cornell, Carnegie Mellon, Northwestern, Texas A&M and Virginia Commonwealth.

Dates

- **Online:** March 9 – April 25, 2015; May 2-10, 2015
- **Onsite Field Study:** April 26 – May 1, 2015

GEORGETOWN UNIVERSITY
School *of* Foreign Service *in* Qatar

Overview

Explore domestic policies in support of international incidents. Utilize a case study based on a coordinated attack in an isolated region. Learn to manage and take courses of action when there are unexpected emergency management challenges due to lack of redundancy and broken supply chains.

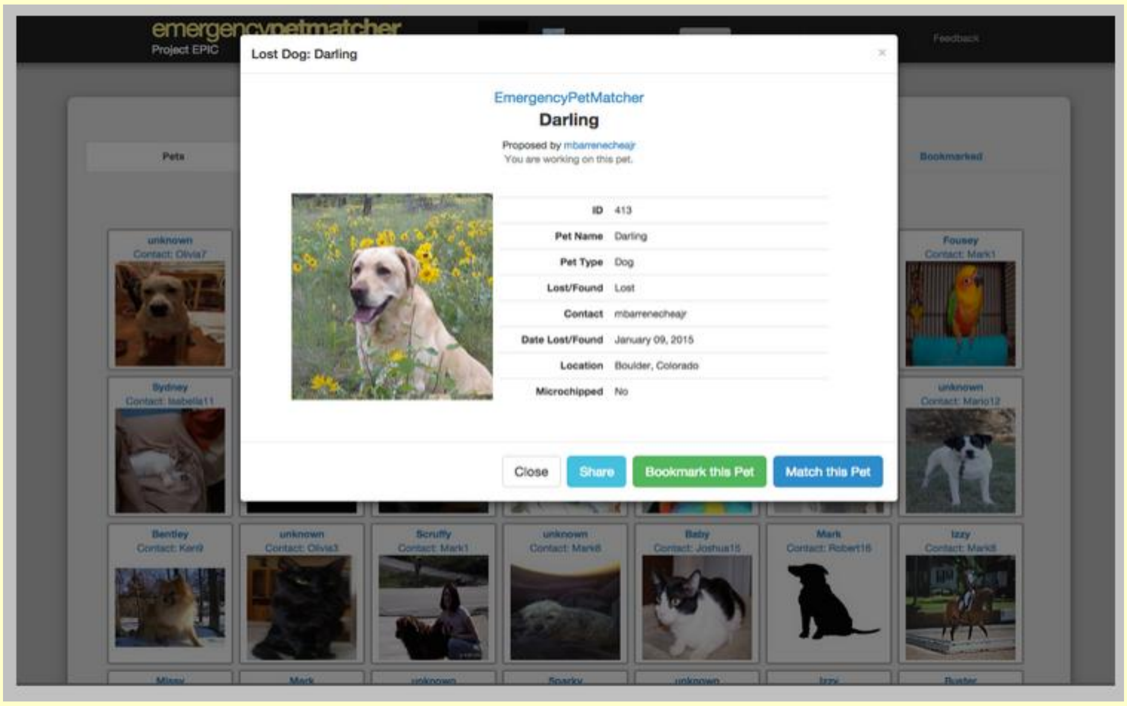
Learning objectives

- Demonstrate an understanding of international and domestic policies governing emergency support of foreign disasters.
- Recognize and respond to multi-dimensional incidents.
- Identify and mitigate challenges associated with disabled or delayed aid, supply chain systems, critical infrastructure and key resources.

▶ **Read more at:** http://qatar.sfs.georgetown.edu

Website Will Help Reunite People with Pets after Disaster

Source: http://www.emergencymgmt.com/disaster/Website-Will-Help-Reunite-People-with-Pets-after-Disaster.html



Lost Dog: Darling

EmergencyPetMatcher

Darling

Proposed by mbarrenecheajr
You are working on this pet.

ID	413
Pet Name	Darling
Pet Type	Dog
Lost/Found	Lost
Contact	mbarrenecheajr
Date Lost/Found	January 09, 2015
Location	Boulder, Colorado
Microchipped	No

In the hours and days after the Black Forest fire erupted June 11, 2013, the Humane Society of the Pikes Peak Region began the task of reuniting people with their misplaced animals — including horses, cats, dogs, cattle and even a parrot separated from their owners.

Shelter and veterinary clinics opened their doors to hundreds of lost animals waiting to be claimed. Peyton resident Cindy McKeon created a Facebook page, Black Forest Fire Lost and Found Pets, where people could post photos of lost pets. Almost two years after the fire, the page is a popular site for lost and found postings.

But a new website created by computer scientists at the University of Colorado at Boulder hopes to make pet-and-owner reunifications during and after disasters even easier. **EmergencyPetMatcher is a one-stop website for lost and found postings, where people can post photos of lost pets and hopefully match them with photos of pets found.** Users of the website can peruse posted photos and look for matches. When a certain number of people suggest a match, an email is generated to the posters of lost and found photos.

Having a system to reunite people with their pets will hopefully mitigate some of the intense trauma of a disaster situation, said Joanne White, a CU Boulder researcher who helped create the website.

"Those most impacted by loss of pets and service animals are also society's most vulnerable — children, the elderly, and the disabled," White said in a news release from the university. "Minimizing the time these people are separated from their animals is an important way to help recovery after a disaster."

The website is intended for use only during a disaster, White said. She declined to discuss the website in greater detail until it goes live — when a disaster occurs.

The website is a part of Project EPIC, a 2009 National Science Foundation initiative that set aside $2.9 million for projects that help with information flow during disasters.

In addition to her work on Emergency PetMatcher, White is working on a way for pet evacuation centers to keep digital records of pets going in and out of shelters. **She also is working on evacuation maps that will help people find the best route to pet evacuation centers,** such as the Elbert County Fairgrounds, during a disaster, according to the university's news release.

> **"Minimizing the time people are separated from their animals is an important way to help recovery after a disaster."**

▶ **Read more on Emergency PetMatcher at:** http://www.emergencypetmatcher.com/

Understanding the ingredients, conditions that cause spot fire ignition

Source: http://www.homelandsecuritynewswire.com/dr20150212-understanding-the-ingredients-conditions-that-cause-spot-fire-ignition

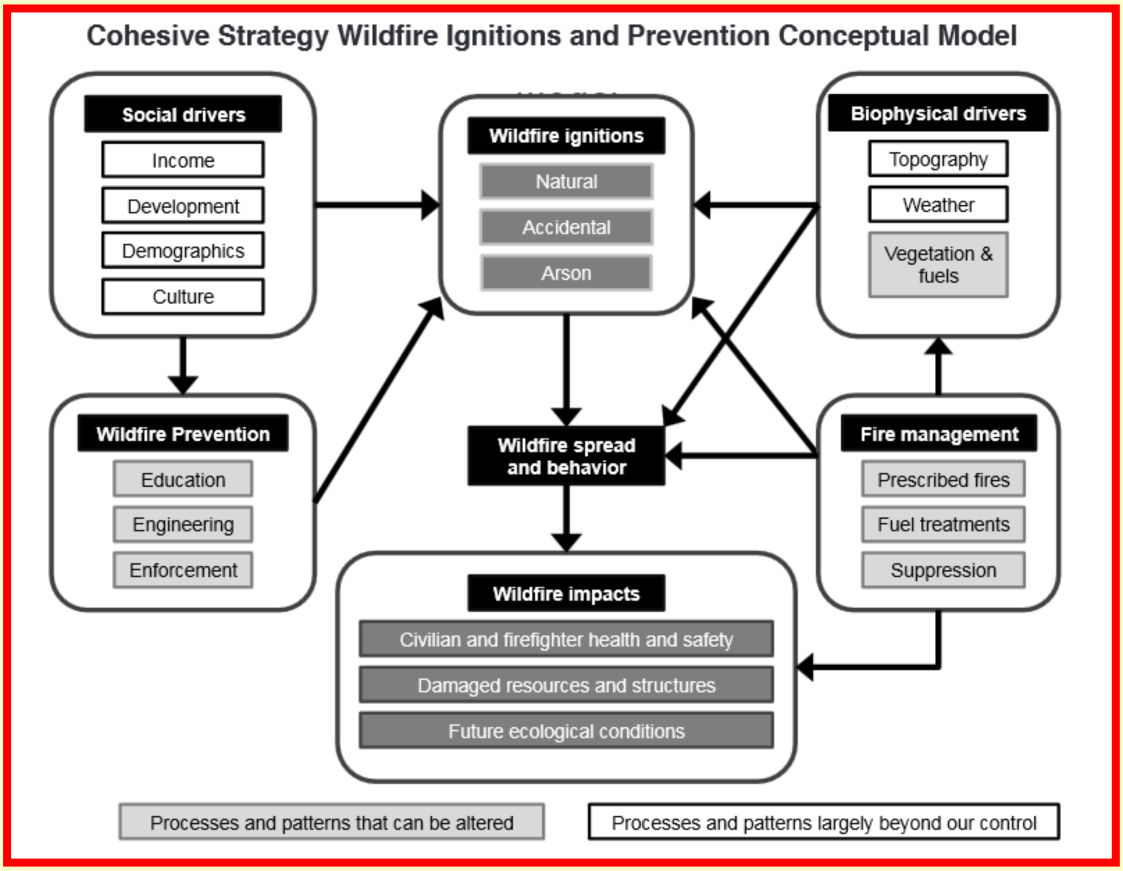
WITCH CREEK FIRE
78
Coronado Hills Fire (100% Contained)
Valley Center
Escondido
Witch Creek Fire
La Costa
78
Lake Hodges
Guajito Fire
78
Ramona
5
Rancho Santa Fe
67
Del Mar
15
FIRE ZONE
56
EVACUATION AREA
ADVISORY EVACUATION
San Vincente Reservoir
805
Witch Creek Fire as of 3 p.m.
67

Hot metal fragments can be created from power lines, overheated brakes, railway tracks, or any other manner of metal-on-metal action in our industrialized society. The particles can reach more than 5,000 degrees Fahrenheit, around the boiling point of most metals.

Although these bits cool as they fall to the ground, they can ignite a flame that quickly spreads if they land on a prime fuel source like pine needles or dry grass.

At least 28,000 fires occur each year in the United States due to hot metal hazards, according to a 2013 U.S. Department of Agriculture report. **For instance, in 2007, a spark from power lines traveled over the wind and landed in dry grass near Witch Creek Canyon in California. Days later, 1,100 homes and 200,000 acres had burned, with $1.8 billion in losses.**

Some human-caused ignitions are on the decrease, such as those caused by cigarettes and arson. Fires that bloom from stray particles, however, continue to be a problem, particularly around mid-sized populations where there is just the right cocktail of civilization and natural fuels.


Cohesive Strategy Wildfire Ignitions and Prevention Conceptual Model
Social drivers
Income
Development
Demographics
Culture
Wildfire ignitions
Natural
Accidental
Arson
Biophysical drivers
Topography
Weather
Vegetation & fuels
Wildfire Prevention
Education
Engineering
Enforcement
Wildfire spread and behavior
Fire management
Prescribed fires
Fuel treatments
Suppression
Wildfire impacts
Civilian and firefighter health and safety
Damaged resources and structures
Future ecological conditions
Processes and patterns that can be altered
Processes and patterns largely beyond our control

An NSF release reports that engineers supported by the National Science Foundation (NSF) are learning what ingredients and conditions cause this type of fire-starting, known as spot fire ignition.

Recipe for ignition

Anyone who has ever tried to light a campfire knows making fire involves a lot of variables. Combustion is essentially a chemical reaction that's determined by temperatures and material makeup. For spot fire ignition, the situation becomes more complex, because environmental conditions play a big role.

"The least understood aspect of the spot fire problem is what happens after a particle lands on a fuel bed," said Carlos Fernandez-Pello, mechanical engineer at the University of California, Berkeley. "The other two parts of the process, particle generation and particle flight, have been relatively well-studied."

Fernandez-Pello and his team mixed metal types and sizes, fuel bed characteristics and wind conditions to see what combinations create fires. Using elegant tabletop experiments, the engineers experimented with a variety of metals and fuels, attempting to replicate real-world conditions.

"Obviously, a study of this complexity is difficult to conduct," Fernandez-Pello said. Brass, stainless steel, copper and aluminum ranging in size from roughly a pencil tip to an eraser were heated to temperatures from 1,100 to 2,200 degrees Fahrenheit. The metals represent those used in activities or events that are known to cause fires, like welding, drilling, metal-cutting and power surges.

In reality, some fragments get even hotter, but the researchers were limited by lab equipment. The metals were then flung into beds of barley grass, pine needles, shredded paper and ground grass and paper — similar to fuels found in the wilderness.

"One of the most difficult experimental challenges was finding ways to make consistent fuel beds, ensuring the same density and moisture content," said Berkeley graduate student researcher

James Urban. "Another difficult part was videotaping the ignition events, which usually happens less than a tenth of a second after the hot particle touches the fuel bed."

We didn't start the fire

The engineers found relatively large fragments could ignite blazes even at low temperatures, if the fuel was of a certain type. Large shards might come from overheated vehicle brakes, bearings or result from sloppy welding.

Small fragments, although more likely to be produced, required higher temperature to ignite fires. The size, shape and arrangement of the individual fuel pieces (for example, needles, grass, shredded paper or grind size) also mattered. The finely ground, dried wood caught fire most easily.

Ignition required a minimum fragment temperature that depended on the fragment's size and the fuel characteristics.

The release notes that the data can help inform computer models that predict fire likelihood based on weather, particle and fuel bed characteristics.

"Enhanced fire spread models could give land managers and government agencies better tools to take preventative measures," Fernandez-Pello said.

Selective clearing around highways and railroads is one form of fire prevention.

Planners often err on the side of caution, understandably. But with more accurate models, more strategic city planning could save trees and prevent forest fires, which is something Smokey can get onboard with.

The results also have uses beyond wildfire prevention.

"The ignition of transportation and rocket fuels share many similarities with wildfire fuels," said Ruey-Hung Chen, program director in NSF's Division of Combustion and Fire Systems, which helped fund the research. "The wildfire ignition research can benefit a wide range of combustion applications."

— Read more in Jeffrey P. Prestemon et al., Wildfire Ignitions: A Review of the Science and Recommendations for Empirical Modeling, General Technical Report SRS-171 (USDA, Forest Service, Southern Research Station, 2013)

Wildland Fire Fighter Uniform Redesigned

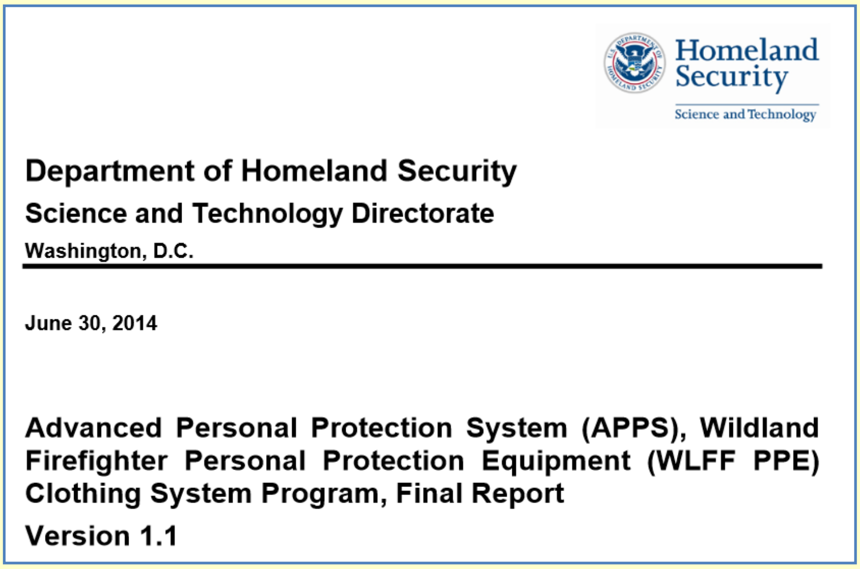
Source: http://www.dhs.gov/science-and-technology/wildland-fire-fighter-uniform-redesigned

Would it surprise you to know that the most common cause of injuries to wildland firefighters is not burns?

When leaders at the California Department of Forestry and Fire Protection (CAL FIRE) noticed their wildland firefighters were experiencing more heat stress injuries—like heat exhaustion and heat stroke—than burn injuries, they wanted to know why and how to prevent them. They soon realized their uniforms were part of the problem. Working with a team at the University of California, Davis, they developed technical and design specifications for a new uniform aimed at increasing the comfort and breathability while maintaining the current level of protection against flames.

In 2011, CAL FIRE approached the Department of Homeland Security Science and Technology Directorate's First Responders Group (FRG) requesting assistance in developing prototype garments. FRG began coordinating with CAL FIRE, California fire departments, and the U.S. Forest Service, who had previously established a working group of wildland firefighters to investigate improvements to their garments to address the heat exhaustion issue. After years of development and testing, the group collectively improved wildland fire advanced personal protection garments, and have published a report on FirstResponder.gov in the hopes of assisting other wildland firefighting organizations.

According to FRG Program Manager William Deso, the group considered improvements to the whole garment ensemble—undergarments, socks, shirt, and pants—during the effort. Deso partnered with the U.S. Army Natick Soldier Systems Center (Natick) to identify a fabric for undergarments that would not melt or drip, would wick away sweat, and would allow the material to breathe. DOD had already developed and issued an advanced fabric for undergarments and socks for deployed military members for use during thermal blasts. This allowed Deso and his team to focus on development of the shirt and pants.



Homeland Security
Science and Technology

Department of Homeland Security
Science and Technology Directorate
Washington, D.C.

June 30, 2014

Advanced Personal Protection System (APPS), Wildland Firefighter Personal Protection Equipment (WLFF PPE) Clothing System Program, Final Report
Version 1.1

“We were able to use garments that the Department of Defense (DOD) had previously developed and that saved time and money,” Deso explained. They then advertised to identify fabric manufacturers that met CAL FIRE’s specifications, and sent samples to North Carolina State University, which manages a leading personal protection equipment (PPE) laboratory, for verification testing.

In addition to developing the new shirt and pants with material that had better breathability, Deso worked with the wildland firefighters to ensure the actual garments were comfortable, more user-friendly, and better suited to their mission.

“We had a clothing designer come to our working group meeting,” Deso recounted. “He talked to them to find out what they wanted and required in order to make the garment functional for their specific tasks. He built a garment that incorporated the specific features identified by the firefighters and wore it to the next meeting so they could look at it on him and evaluate it. They provided input; he made adjustments.”

It took three iterations, but the wildland firefighters finally had the design they wanted. Deso distributed the garments and began testing in the field in late 2012, and received feedback from firefighters on the garments’ performance. Based on that feedback, FRG tweaked the uniform and distributed a limited number of a second-generation version for additional testing in 2013. Deso and his team documented the process, the fabric, and the garments’ performance in a report to allow other wildland firefighters, not just CAL FIRE, to benefit from the development effort.

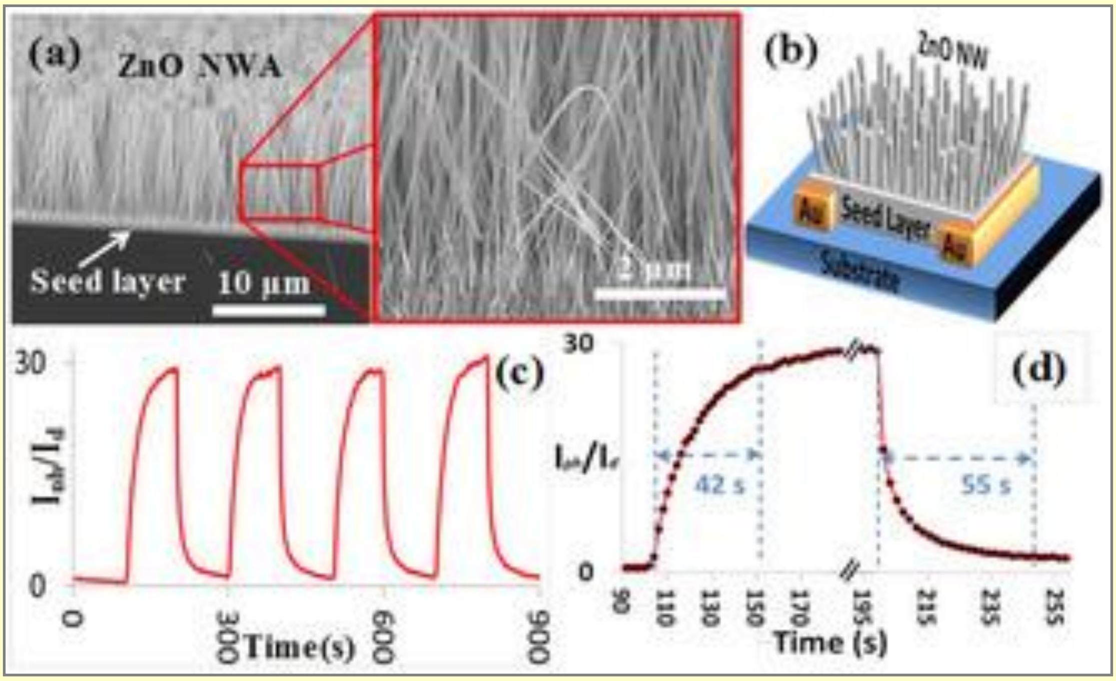
Deso and the team hope that they can transition the PPE into the commercial market. Vendors are already indicating interest in making this a possibility by requesting the report and patterns. “We hope folks will use the report and that wildland firefighter procurement officials will compare what they currently have to what’s available. These new garments offer the same level or better of protection and are much more comfortable.”

▶ **Read the report at:** http://www.firstresponder.gov/TechnologyDocuments/APPS%20-%20WLFF%20PPE%20FINAL%20REPORT%20%282%29.pdf

Fire detectionImproved fire detection with new ultra-sensitive, ultraviolet light sensor

Source: http://www.homelandsecuritynewswire.com/dr20150218-improved-fire-detection-with-new-ultrasensitive-ultraviolet-light-sensor

Feb 18 – **A new study published in *Scientific Reports* has discovered that a material traditionally used in ceramics, glass and paint can be manipulated to produce an ultra-sensitive UV light sensor, paving the way for improved fire and gas detection.**



(a) SEM images, (b) schematic diagram, (c), and (d) the photoresponse characteristics of the ZnO NWA detector.

Researchers at the University of Surrey's Advanced Technology Institute manipulated zinc oxide, producing nanowires from this readily available material to create an **ultra-violet light detector that is 10,000 times more sensitive to UV light than a traditional zinc oxide detector.**

A University of Surrey release reports that currently, photoelectric smoke sensors detect larger smoke particles found in dense smoke, but are not as sensitive to small particles of smoke from rapidly burning fires.

Researchers believe that this new material could increase sensitivity and allow the sensor to detect distinct particles emitted at the early stages of fires, paving the way for specialist sensors that can be deployed in a number of applications.

"UV light detectors (photo, right) made from zinc oxide have been used widely for some time but we have taken the material a step further to massively increase its performance," said Professor Ravi Silva, co-author of the study and head of the Advanced Technology Institute.

"Essentially, **we transformed zinc oxide from a flat film to a structure with bristle-like nanowires, increasing surface area and therefore increasing sensitivity and reaction speed.**"

The team predicts that the applications for this material could be far-reaching. From fire and gas detection to air pollution monitoring, they believe the sensor could also be incorporated into personal electronic devices – such as phones and tablets — to increase speed, with a response time 1,000 times faster than traditional zinc oxide detectors.

"This is a great example of a bespoke, designer nanomaterial that is adaptable to personal needs, yet still affordable. Due to the way in which this material is manufactured, it is ideally suited for use in future flexible electronics — a hugely exciting area," added Professor Silva.

— Read more in Mohammad R. Alenezi et l., "On-chip Fabrication of High Performance Nanostructured ZnO UV Detectors," Scientific Reports *5, Article number: 8516 (17 February 2015)(http://www.nature.com/srep/2015/150217/srep08516/full/srep08516.html)*

Study: Terror attacks offer insights for first responders

Source: http://www.buffalo.edu/news/releases/2015/02/027.html#sthash.IGoCFvK3.dpuf

Security services survey a destroyed room inside the Taj Mahal Palace and Tower Hotel after the armed siege on Nov. 29, 2008, in Mumbai, India. The city of Mumbai was rocked by multiple coordinated terrorist attacks that targeted locations popular with foreigners, late on Nov. 26, killing at least 166 people. (Credit: Julian Herbert)

When terrorists strike, emergency workers who have the proper training, information access and a positive work environment will make better decisions, according to research from the University at Buffalo School of Management.

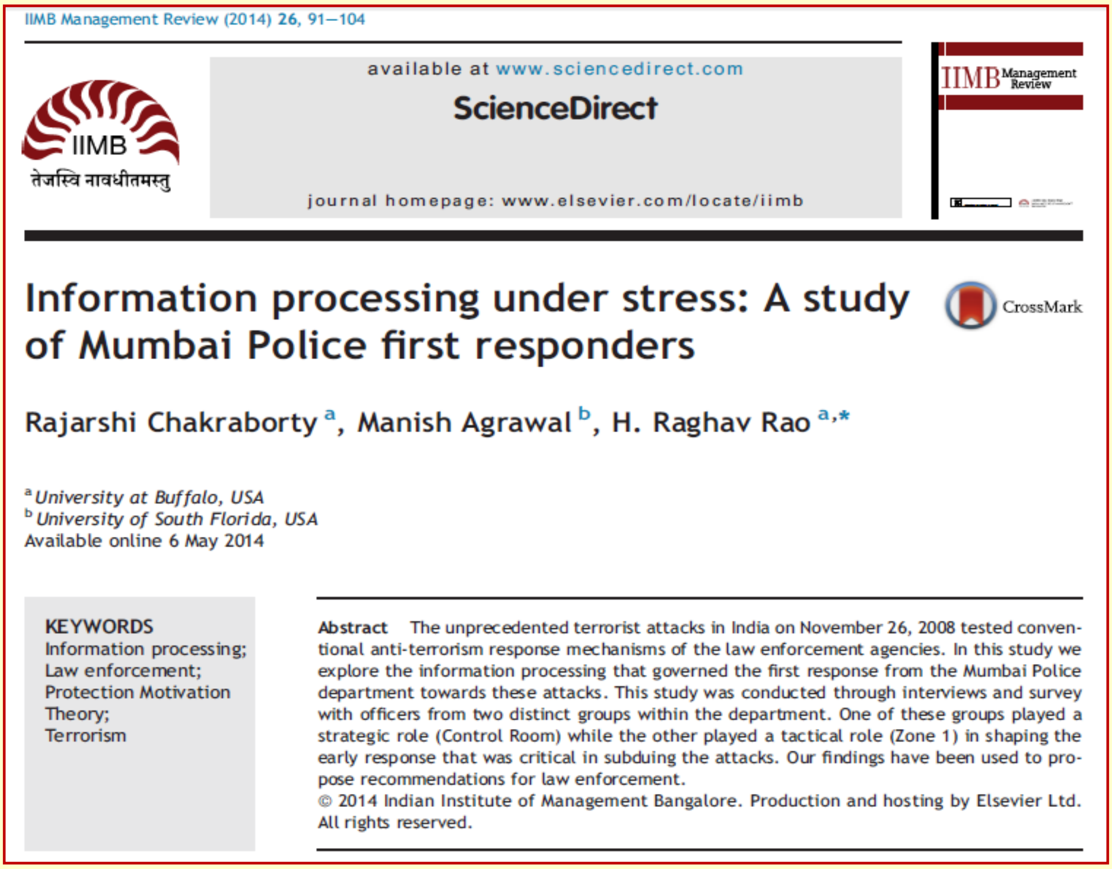
Published in IIMB Management Review, the study was prompted by the terrorist attacks in Mumbai, India, on Nov. 26, 2008, that killed 166 people and are often referred to as India's 9/11.

The research, co-authored by H. Raghav Rao, PhD, SUNY Distinguished Service Professor, Management Science and Systems Department in the UB School of Management, focused on understanding the motivation and decision-making process of first responders during the attacks.

"An officer in the police department, whether in the control room or in the field, makes many critical decisions during a situation like the Mumbai terrorist attacks," says Rao. "Each of these decisions is driven by a motivation, which is usually derived from knowledge of the situation at hand."

"Many callers to the Mumbai Police control room during the terrorist attacks didn't know the street names in their immediate neighborhood."

H. Raghav Rao, SUNY Distinguished Service Professor, Department of Management Science and Systems; University at Buffalo



IIMB Management Review (2014) 26, 91–104

available at www.sciencedirect.com

ScienceDirect

journal homepage: www.elsevier.com/locate/iimb

Information processing under stress: A study of Mumbai Police first responders

Rajarshi Chakraborty [a], Manish Agrawal [b], H. Raghav Rao [a,*]

[a] University at Buffalo, USA
[b] University of South Florida, USA

Available online 6 May 2014

KEYWORDS
Information processing;
Law enforcement;
Protection Motivation Theory;
Terrorism

Abstract The unprecedented terrorist attacks in India on November 26, 2008 tested conventional anti-terrorism response mechanisms of the law enforcement agencies. In this study we explore the information processing that governed the first response from the Mumbai Police department towards these attacks. This study was conducted through interviews and survey with officers from two distinct groups within the department. One of these groups played a strategic role (Control Room) while the other played a tactical role (Zone 1) in shaping the early response that was critical in subduing the attacks. Our findings have been used to propose recommendations for law enforcement.

The study analyzed surveys from 31 Mumbai Police officers who were involved in the immediate response to the terrorist attacks. In addition, they conducted interviews with 15 middle- to high-ranking officers who directly assisted in the efforts to mitigate the effects of the attacks.

The researchers analyzed the information gathered during these surveys and interviews and offer the following recommendations to prepare first responders for terrorist attacks:

- **Remove barriers to information sharing.** When responders have timely access to important information in a crisis, they have increased motivation to take action.
- **Improve training.** Improved training in how to deal with, assess the severity of and quickly respond to crisis situations will lead emergency workers to more helpful actions and decisions.
- **Establish an optimistic work environment.** Hopefulness improves the likelihood that responders will take positive steps to alleviate crisis situations.
- **Create a decision support system.** Officers should be trained to pick up important information, make decisions from that information and be provided with the tools they need to communicate those decisions to the necessary personnel.

The authors also recommend a number of ways Mumbai Police can improve information sharing during such a crisis.

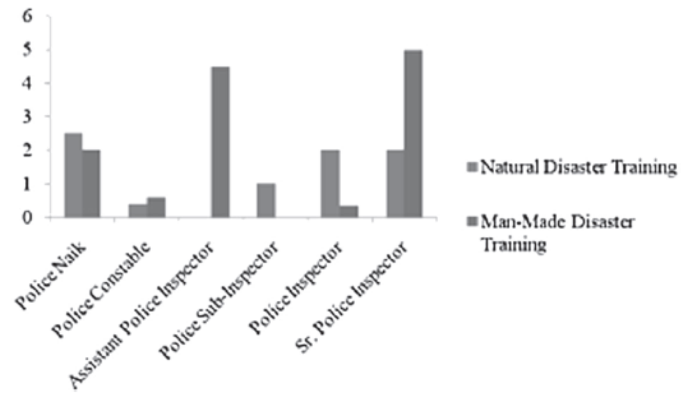


Figure 2 Amount of disaster training — Mumbai Police department.

"Many callers to the Mumbai Police control room during the terrorist attacks didn't know the street names in their immediate neighborhood," says Rao. "A campaign to educate residents about these names would help first responders more effectively reach people in need in the future."

In addition, the study recommends sending private closed-circuit television signals to police, broadcasting information across police zones and sending official social media alerts to dispel rumors. Officials also should implement a system of alert levels that define operating procedures under different terrorist threats.

Rao collaborated on the project with Manish Agarwal, PhD, associate professor of information systems and decision sciences in the University of South Florida Muma College of Business, and Rajarshi Chakraborty, doctoral student of Management Science and Systems in the UB School of Management. The study was supported by a grant from the National Science Foundation.

The UB School of Management is recognized for its emphasis on real-world learning, community and economic impact, and the global perspective of its faculty, students and alumni. The school also has been ranked by Bloomberg Businessweek, the Financial Times, Forbes and U.S. News & World Report for the quality of its programs and the return on investment it provides its graduates. For more information about the UB School of Management, visit mgt.buffalo.edu.

CCTV feeds to control room, ready availability of blueprints of large buildings to police, and training of police in use of fire extinguishers: Most of the attacked installations in the city had closed circuit TV setups. However, these were not shared with the police. Organisations that are likely to be targetted should be encouraged to share CCTV feeds with Mumbai police to protect the security interests of these organisations. To protect business interests, sharing may be limited to information that is most helpful from a security perspective. However, it may be useful to have a mechanism in place so that in case of an emergency, more information can be shared based on needs. Further, blueprints and building floor plans (including waterlines and fire exits) of all large buildings should be readily (but securely) available to the police. Police should also be trained in using fire extinguishers. Blueprints and floorplans[3] should be scanned and made available under a secure server to the police. In addition the blueprints giving easy exits should be easily visible to everyone in the building.

▶ **Read the full paper at:** http://www.sciencedirect.com/science/article/pii/S0970389614000299

New climate change projections for Australia

Source: http://www.homelandsecuritynewswire.com/dr20150127-new-climate-change-projections-for-australia

Jan 27 – CSIRO and the Australian government's Bureau of Meteorology the other day released climate change projections for Australia which provide updated national and regional information on how the climate may change to the end of the twenty-first century.

CSIRO says that the projections are the most comprehensive ever released for Australia and have been prepared with an emphasis on informing impact assessment and planning in the natural resource management sector. Information has been drawn from simulations based on up to forty global climate models.

CSIRO and Bureau researchers have confirmed that most of the changes observed over recent decades will continue into the future.

"There is very high confidence that hot days will become more frequent and hotter", CSIRO principal research scientist, Kevin Hennessy said.

"We also have very high confidence that sea levels will rise, oceans will become more acidic, and snow depths will decline."

"We expect that extreme rainfall events across the nation are likely to become more intense, even where annual-average rainfall is projected to decline."

In southern mainland Australia, winter and spring rainfall is projected to decrease, but increases are projected for Tasmania in winter.

For the rest of Australia, naturally occurring fluctuations in rainfall patterns will dominate over trends due to climate change until 2030, after which the trends associated with climate change will begin to emerge.

By 2090, winter rainfall is expected to decrease in eastern Australia.

Southern and eastern Australia are projected to experience harsher fire weather, while tropical cyclones may occur less often, but become more intense.

"This research has been strongly aligned with the needs of Australia's natural resources sector", Hennessy said. "Other researchers are using this information to assess potential impacts and management options."

Projected changes will be superimposed on significant natural climate variability.

Observed climate information indicates that Australian average surface air temperature has increased by 0.9° C since 1910, and many heat-related records have been broken in recent years. Sea level has risen about 20 cm over the past century.

The Bureau of Meteorology has observed that since the 1970s, northern Australia has become wetter, southern Australia has become drier, the number of extreme fire weather days has increased in many places, and heavy rainfall has accounted for an increasing proportion of annual-total rainfall.

Snow depths have declined since the 1950s and cyclone frequency seems to have declined since the 1980s.

▶ **The reports can be downloaded here.**

— Read more in State of the Climate 2014 (Australian Government, Bureau of Meteorology, 2015); and Climate Change in Australia, Technical Report (2015)

Norway Defense Minister Urges Deterring Hybrid Warfare Threat

Source:http://sputniknews.com/military/20150206/1017902690.html#ixzz3R4bIfljk

The danger of hybrid warfare should be taken seriously, Norway's Defense Minister Ine Eriksen Soreide said Friday at the Munich Security Conference.

"We have to take it seriously. It has been a long-going discussion within NATO and other institutions," Soreide said in Germany, adding that it was important to decide on an adequate response.

Hybrid warfare refers to a military strategy that uses a broad range of tools, combining conventional warfare with cyberwarfare, information warfare and guerrilla warfare. It may also be used to describe attacks using weapons of mass destruction, such as chemical, biological and nuclear weapons.

Soreide (photo) stressed that more investment in defense and security was needed to address the challenge. Norway has been stepping up its investment in intelligence and high-end capabilities, she added.

"And the reason we are doing all this – and I think that is important to remember – is that we need to be able to counter a full spectrum of threats," the Norwegian military chief said.

"Over the course of the [Crimean] crisis, Russian leaders denied any active involvement but sent irregular forces dubbed 'little green men,' spread propaganda and encouraged local unrest, assembled regular forces at the border, and engaged in diplomacy trying to keep up the narrative that Moscow was not a party to the conflict," the expert panel said in a report.

The republic of Crimea voted March 2014 rejoin Russia amid the worsening security situation in mainland Ukraine following a February 2014 coup. The decision was condemned by the West. US and EU leaders have accused Russia of active military involvement in the unfolding Ukrainian crisis, and have been considering whether to supply the government in Kiev with lethal aid.

How a Warming Climate Impacts Public Health

By David Raths

Source: http://www.emergencymgmt.com/health/How-Warming-Climate-Impact-Public-Health.html

Feb 03 – It may seem counterintuitive to make a connection between a warming planet and the huge snowfall totals that hit Buffalo, N.Y., in November, but these dramatic storms are happening at least in part because the world is warmer, scientists say.

"There is an influx of Arctic air into Buffalo because the Arctic is warm," said John Balbus, senior adviser for public health at the National Institute of Environmental Health Sciences. The water temperatures in the Bering Sea are running way above what are usual, the air temperatures are higher and it displaces the usual patterns, he added.

As researchers study climate change, one area getting more attention recently is the impact of climate variability on public health. Greater climate variability means regions of the country can expect to see new types of human health hazards, which will lead to more public health emergencies.

"Places that haven't had to deal with certain kinds of phenomena, like searing heat in Minnesota or in coastal Washington, need to start developing plans to prepare for that, because they will have to deal with it," Balbus said.

The Centers for Disease Control and Prevention (CDC) has identified several ways public health will be affected as temperatures rise, and many of them could have a direct impact on emergency management and response:

- increasing deaths and illnesses from heat stress;
- increasing risk of injuries and illnesses due to extreme weather events, such as storms and floods;
- more respiratory and cardiovascular illness and deaths caused by smoke from heat- and drought-related wildfires, as well as changes in air pollution, particularly ozone smog;
- changes in the rates and ranges of infectious diseases carried by insects or in food and water;
- threats to the safety and availability of food and water supplies; and
- greater levels of mental and emotional stress in response to climate change and extreme weather-related emergencies.

George Luber, an epidemiologist and the associate director for global climate change in the Division of Environmental Hazards and Health Effects at the CDC's National Center for Environmental Health, said researchers are seeking to understand the key pathways through which health will be compromised. There are direct impacts, such as storms, extreme weather, heat waves and air quality problems, but there are also indirect effects climate change will have, including the abundance and distribution of vector-borne diseases.

Climate change will affect the cumulative exposure people have to some impacts, Luber explained. “If you get heat stroke once, your sensitivity to heat is much higher the next time around,” he said. “Multiple heat waves have a cumulative effect. Multiple cumulative exposures to bad air mixed with high temperatures mixed with ozone have a death-by-a-thousand-cuts impact. But in addition to that, you have the potential for more complex emergencies.”

The magnitude of climate change-related events is projected to get much bigger, and storms will stress the capability of response systems to manage them. “The potential for multiple disasters within a disaster really exacerbates public health issues,” Luber said. “A loss of electricity affects those on durable medical equipment. We do see a spike in mortality during power outages. Those systems — communications for EMS, transportation for egress from storms, power — when those go down, public health is affected. And those types of incidents are expected to increase in frequency and magnitude from storms. That is of critical importance.”

Luber reiterates Balbus’ comment about regions needing to prepare for surprises and anomalous weather events. Profound changes in ecology lead to the potential for the emergence of pathogens in areas where they have never been seen before. “We are seeing a food-borne illness, paralytic shellfish poisoning, in Alaska that extended the northernmost range 1,000 kilometers,” he said. And he pointed to the 2003 heat wave in Europe, which killed approximately 70,000 people, and for which public health officials there were unprepared. “In subsequent heat waves, they learned their lesson,” Luber said. “It drove home to them that they need to prepare for an event they have never experienced before.”

Regional public health officials are making the connection between climate change and chronic health conditions. **The increase in ground-level ozone causes airway inflammation that can damage lung tissue, said Anne Kelsey Lamb, director of the Oakland, Calif.-based Regional Asthma Management and Prevention (RAMP), a project of the Public Health Institute.** “We also see climate change is leading to an increase in particulate matter, which are tiny particles, which, if inhaled, can damage the lungs and cause chronic breathing problems,” she said.

Another way climate change is impacting asthma is through increasing the length of ragweed pollen season, which is a significant asthma trigger. “We see that this is already happening and is only going to get worse,” Lamb said.

RAMP has been working with other Public Health Institute projects toward the goal of increasing public health engagement in climate action. “We are recognizing that climate change is one of the most significant public health issues of our time, and we want to see the public health community increasing the level of engagement with this issue,” Lamb said. “Asthma is just one example, and it is the one my organization is most focused on, but there are so many other ways that climate change is already impacting public health. We want to see the public health community become more engaged.”

There are ways that the whole array of public health strategies — policy advocacy, surveillance and monitoring, health education and case management — can integrate climate change, Lamb said. “Even recognizing the financial constraints of many people working in public health, we would recommend there are ways they can integrate climate change into what they are already doing as part of their everyday job.”

The release of the third annual National Climate Assessment in 2014 was a milestone for public health, said Georges Benjamin, executive director of the American Public Health Association.

“The significance of the National Climate Assessment is the recognition that climate change is here now,” he said. “We have been hearing that it is coming. Well, people now realize that it is already here and affecting every region of the nation.”

Public health agencies need to think about how they are going to respond, Benjamin said. “They have to know where their vulnerable citizens are so that when there is a severe event, they can respond to their needs,” he said. “When the power goes off, they can prioritize people who will need help right away because they are at home with electronics-dependent equipment.”

More work needs to be done around systems preparedness and doing out-of-the-box thinking about cascading failures, Benjamin said. “We know that in Hurricane Sandy, EMS units had to move out of firehouses because of flooding. What do you evacuate to and maintain response capacity? What is the backup plan if 911 goes down?”

Many states and some cities are starting to do vulnerability assessments as part of the Climate-Ready States and Cities Initiative, which Luber’s office at the CDC oversees. With federal grant funding, 16 states and two cities (San Francisco and New York) are going through a five-step process to anticipate health effects by applying climate science to predict health impacts and prepare flexible programs.

The program, called BRACE (Building Resilience Against Climate Effects), takes a hazards assessment approach. “It is guided by principles of adaptive management, which is an iterative, learning-based process,” Luber said.

The first step is projecting current climate hazards into the future. States identify their principal hazards, such as heat waves and floods, and use climate models to project how those will change in the future. North Carolina, for instance, would look at flood plains, coastal zones and urban heat islands, and which populations are most vulnerable, as well as risk factors for exposures.

The assessment would also look at rates of respiratory problems, water-borne disease incidents, septic systems and other aggregations of risk to project disease burden. Officials look at the current health profile of the state and project how that could change in the future. “The next question is: Which ones can we do something about now?” Luber said. “They identify which interventions would have the most impact and work to put those in place. They are also building capacity to track health outcomes over time.”

For example, the BRACE program at the Florida Department of Health collaborated with the University of South Carolina Hazards and Vulnerability Research Institute to assess hurricane winds, storm surge, sea-level rise, drought and wildfires. To quantify social and medical vulnerability to these hazards, they used a Social Vulnerability Index and Medical Vulnerability Index linked to hazard maps to display the intersection of vulnerabilities and hazards throughout the state.

Some states are trying new technologies and approaches. For instance, Vermont is using crowdsourcing and a Web-based tracking tool to identify the presence of ticks.

A 2014 report in the Journal of the American Medical Association notes that in response to heat waves, “cities with investments in early warning and response programs have seen some success. For example, after Milwaukee implemented an extreme heat conditions plan following 91 fatalities during the 1995 heat wave, a subsequent heat wave in 1999 resulted in only 10 deaths, or 49 percent less than expected.”

Benjamin said it is important for public health agencies to form tighter partnerships with other emergency response organizations. “The time to plan is now,” he stressed. “In the middle of a disaster is not the time to exchange business cards.” Agencies need to plan and drill together and understand each other’s capabilities, he added. They should provide redundancies in systems and make sure they have adequate communications capacity. “We have lots of multijurisdictional responses to things, and frequently the responders can’t talk to each other.”

"The time to plan is now. In the middle of a disaster is not the time to exchange business cards."

Even primary care providers should begin talking to patients about emergency preparedness, Benjamin said. Doctors can help people think through how they should prepare for emergencies, especially if they have a medical condition that requires some urgency. “In the hospital settings, we have seen several cases where patients had to be evacuated. We need to be more imaginative about what can go wrong.” While there were some improvements after hurricanes

Katrina and Rita, he said, there were evacuations again during Sandy.

Balbus is leading an initiative called Sustainable and Climate-Resilient Healthcare Facilities, a public-private partnership developed to ensure that facilities such as hospitals, nursing homes and dialysis centers are getting information to help them prepare for their role in extreme weather situations. "Having to move patients in a storm is a huge issue," he said. "We've seen very straightforward, low-tech things cause problems, like getting an emergency generator out of a basement during a flood." The goal is to look at innovative architectural designs for new structures as well as doing vulnerability assessments on existing ones.

Benjamin called it a tragedy that climate change has become unnecessarily political. "Climate change, hurricanes and tornadoes don't know political parties or pick victims.

People need to follow the science. Shame on us if we can't put aside the politics on this," he said. "The scientific community is clear about it. There was a time, not that long ago, when this was a bipartisan issue. We are hoping it will get back to that."

***David Raths** is a contributing writer for* Emergency Management *magazine.*

BUSINESS CONTINUITY

Cyber-attacks become top business continuity threat

By Jimmy Nicholls

Source: http://www.cbronline.com/news/security/cyber-attacks-become-top-business-continuity-threat-4513925

Feb 17 – Cyber-attacks are now regarded as the top threat to business continuity, according to a study by the Business Continuity Institute (BCI).

An annual survey by the firm showed that four-fifths of business continuity managers were afraid that they would be victim of a cyber-attack, just above concerns around unplanned IT outages and data breaches.

Lyndon Bird FBCI, technical director at the BCI, said: "The world faces diverse problems from cybercrime and political unrest to supply chain vulnerabilities and health hazards. This report shows the vital importance of business continuity professionals understanding such trends.

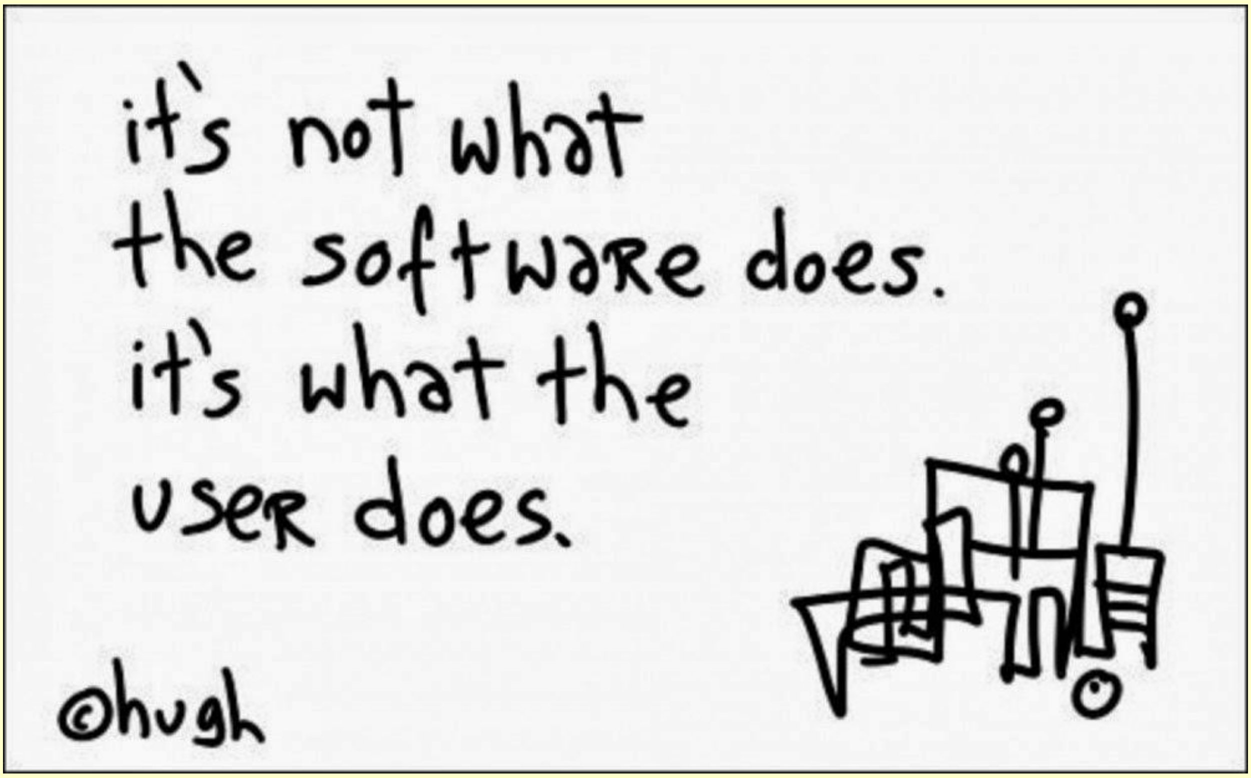
"No longer can those working in the field believe they can resolve all their problems themselves. As an industry we must work together with our fellow practitioners to deal with the complexity of these threats."

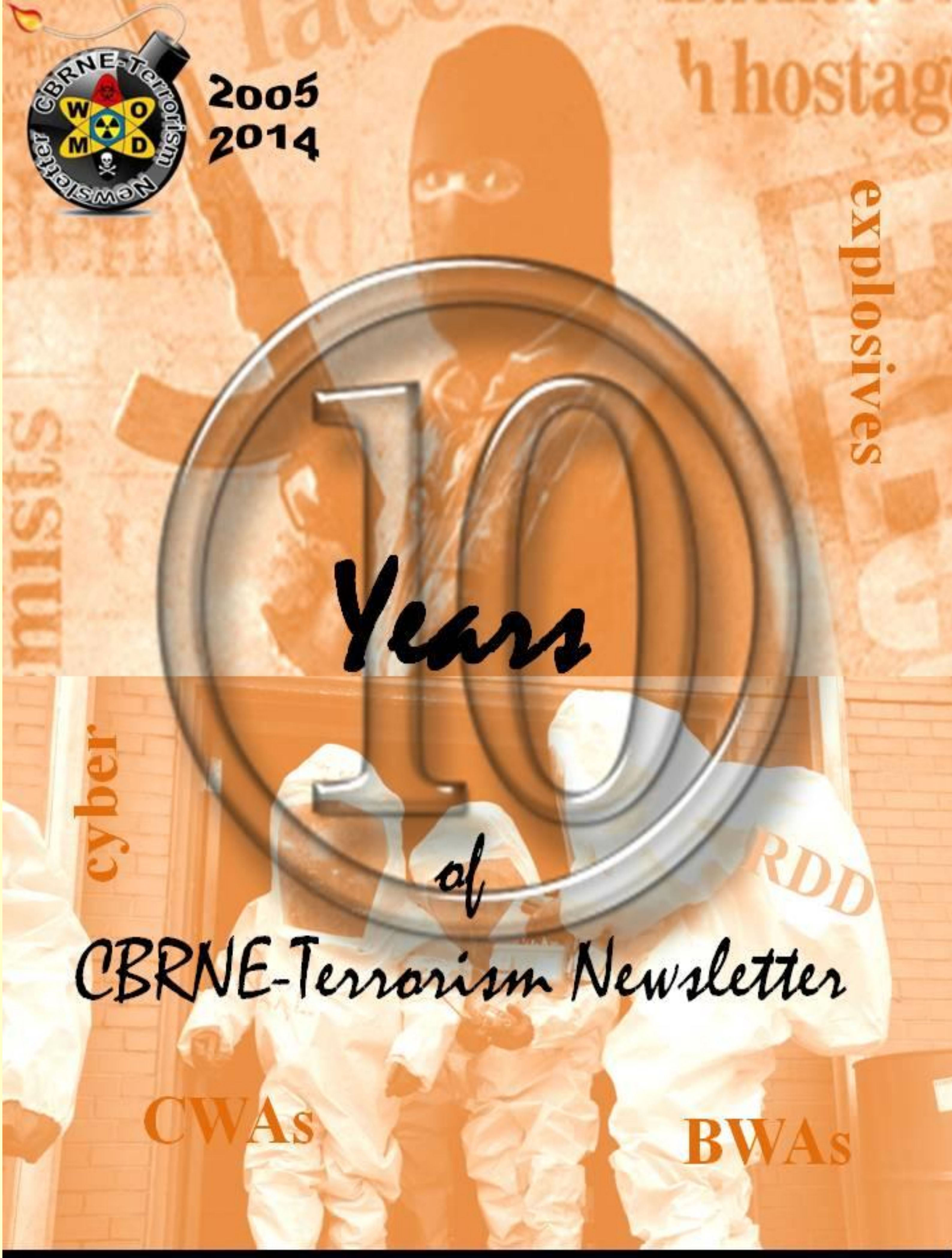
The report, titled Horizon Scan, also showed a decline in the use of trend analysis for those responsible for business continuity, with a fifth of firms not investing in protective discipline whilst a similar amount were not using trend analytics at all.

Analysis of small businesses also showed only half were adhering to standards for business continuity, though the lack of historical data meant it was unknown what direction the trend was moving in.

"Globalisation has brought the world's conflicts, epidemics, natural disasters and crime closer to home," said Howard Kerr, chief executive of the British Standards Institution, which also worked on the report.

"Failing to apply best practice leaves organizations and their employees, business partners and customers at risk."





2005
2014

10 Years of CBRNE-Terrorism Newsletter

WE have to be lucky all the time. THEY have to be lucky only once!