November 2015

CBRNE NEWSLETTER TERRORISM

E-Journal for CBRNE & CT First Responders

10 years

Pakistan Will Be World's Fifth Largest Nuclear Power by 2025, Report Says

Source: http://time.com/4082776/pakistan-report-nuclear-weapons-fifth-largest-2025/
Oct. 22, 2015

FAROOQ NAEEM—AFP/Getty Images A Pakistani commando (R) looks on as Ghauri intermediate-range missiles capable of carrying nuclear warhead are transported on launchers during the National Day parade in Islamabad, 23 March 2005.

Pakistan is on track to become the world's fifth largest nuclear power by 2025, according to a report released by a U.S.-based independent research organization on Monday.

The report by Chicago-based think tank Bulletin of the Atomic Scientists predicts that the South Asian nation's stockpile of nuclear weapons will more than double over the next decade from its current arsenal of 110 to 130 warheads.

The report's estimate of 220 to 250 warheads based on "Pakistan's performance over the past 20 years and its current and anticipated weapons deployments" could potentially place it just behind the U.S., Russia and France, and nearly on par with China's current stockpile of 250.

The report's release coincides with Pakistani Prime Minister Nawaz Sharif's visit to the U.S. this week, where Reuters reports he is expected to tell President Barack Obama that limits on Pakistan's use of small tactical nuclear weapons are unacceptable. Such weapons, Pakistan says, are essential to any potential conflict with its neighbor and fellow nuclear power India — with which it has fought three wars since their independence in 1947.

While India's current nuclear doctrine espouses a strict "no-first use" policy, Pakistan's does not provide any such guarantee — particularly when it comes to India.

"Pakistan's nuclear program is … India-centric," a Pakistani security official familiar with the country's nuclear program told Reuters. "And it exists to make war a nonoption."

The Bulletin report recognizes this fact as well, highlighting two main considerations while analyzing Pakistan's projected nuclear expansion.

"Two key factors," it says, "will be how many nuclear-capable launchers Islamabad plans to deploy, and how much the Indian nuclear arsenal grows."

Japan should restart more nuclear power plants

By Seth Baum

Source: http://thebulletin.org/japan-should-restart-more-nuclear-power-plants8817

In August, a Japanese utility company restarted the Sendai nuclear power plant, sparking controversy and protests. Like the rest of the country's nuclear power generators, Sendai was shut down following the 2011 Fukushima disaster, in which a powerful earthquake and tsunami caused three reactors to melt down. Sendai is the first and so far only nuclear plant to reopen, and

with memory of the catastrophe still fresh, the public outcry is hardly surprising. Applications by other plants to relaunch are also facing legal challenges.

Restarting Japan's nuclear power plants is, however, the right decision, provided they can pass strict new safety checks instituted since Fukushima. The reason is simple: While nuclear power comes with risks, the primary alternative comes with bigger ones.

Turning off nuclear power requires either turning on another power source, or using less electricity. Japan has done both. Its total energy consumption is down 10 percent since 2010 due to the nuclear phase-out, but use of natural gas, a source of greenhouse gas emissions, is up 19 percent, and use of coal, which is even more harmful to the environment, is up 2 percent. (The data is available here.) Japan is now building 45 new coal power plants, but if it turned its nuclear power plants back on (except of course for the damaged Fukushima facilities), it could cut coal consumption in half. **And coal poses more health and climate change dangers than nuclear power.**

The primary harm caused by nuclear accidents is increased cancer risk from released radiation. But the radiation levels from Fukushima are so low that the cancer increase will be barely noticeable, and may not happen at all. To be sure, the radiation exposure would have been worse if the prevailing winds did not blow most of the radiation out to the Pacific. But as with the Chernobyl catastrophe in 1986, the Fukushima disaster caused more harm from overreaction to the radiation than from radiation itself. That's partly because excessive evacuations can cause more deaths than they prevent. The anti-radiation stigma also levied a psychological toll, with some healthy people committing suicide. In Chernobyl, as many as 100,000 unnecessary abortions may have been performed due to fears of radiation's impact.

Another nuclear power plant accident in the near future is, moreover, extremely unlikely. It is normal to pay attention to disasters that are fresh in our memory and overestimate the risk of another; psychologists call this the recency effect. But nuclear plant accidents do not come in bunches. According to the International Atomic Energy Agency (IAEA), the **Fukushima accident is only the second Level 7 major accident in nuclear power history, the first being the Chernobyl disaster 29 years ago**. If anything, we should expect the probability of another accident in Japan to be smaller now because so many people are paying attention to the plants and the institutions overseeing them.

Meanwhile, coal plants also damage human health, through asthma, bronchitis, cancer, and other illnesses. The difference is that nuclear plants only harm health following rare accidents, whereas working coal plants do so all the time. So by switching from nuclear to coal, Japan is rejecting a small chance of increased cancer in favor of a guaranteed increase in cancer and other maladies. In fact, one study found that coal causes 387 times more deaths per unit of energy than nuclear power. Since coal is also more expensive for Japan (as even critics of the nuclear restart have pointed out), restarting the nuclear plants appears to be very much in the country's national interest.

It is also in the world's interest. **Of all major energy sources, coal is the worst emitter of greenhouse gases, warming the planet more per unit of electricity than anything else.** According to the Intergovernmental Panel on Climate Change, nuclear power plants emit about one-tenth to one-twentieth of the greenhouse gases that coal plants do, with emissions coming mainly from power plant construction and uranium mining. And climate change, which affects the entire planet for millennia, is a bigger danger than nuclear plant accidents, which affect small regions for a few years.

True, nuclear waste can also survive for millennia, but carbon dioxide emissions are worse for both humanity and nature. They spread worldwide, whereas nuclear waste is confined to a fixed location. (A regulatory double-standard currently exists across the world, in which the nuclear sector is required to sequester its waste for the long term, but the fossil fuel sector is not.) At worst, nuclear waste can render small regions uninhabitable, though it's worth noting that the Chernobyl area now has flourishing wildlife. Carbon dioxide emissions, however, will ruin far more land via sea-level rise and other changes to the landscape such as desertification, invasive species, and ecological regime shifts. At worst, carbon

dioxide emissions could render large portions of Earth's surface uninhabitable for mammals: When temperature and humidity are so high that we cannot perspire to regulate our body temperatures, we overheat and die.

No accounting of nuclear power risks would be complete without considering the possibility that it can contribute to the spread of nuclear weapons. Since nuclear power can facilitate development of the materials and technology required to make such weapons, ordinarily one might expect the risk to increase with more power plants. However, due to a unique mix of technological and political factors, today, more nuclear power in Japan would actually lower the risk of nuclear weapons proliferation.

The reason for Japan's unusual situation comes from the fact that it is the only non-nuclear-armed state that reprocesses plutonium. The intent is to plow the material back into nuclear reactors to make more electricity, but Japan's resulting plutonium stockpile is now big enough to produce thousands of nuclear weapons. **In 2016, the country plans to open the much-delayed Rokkasho Reprocessing Plant, which, in the absence of operational nuclear plants to consume the resulting plutonium, would increase the stockpile even further.**

Japan currently has 47 metric tons of separated plutonium, 11 at home and 36 in France and the United Kingdom. If all of its nuclear power plants capable of consuming plutonium were restarted, and the Ohma plant, now under construction, were completed, Japan could consume about 4 metric tons per year—in principal drawing down its domestic supply within three years and its international supply in nine. However, if Rokkasho opens it will produce about 4.5 metric tons per year, exceeding Japan's ability to use up its supply. And, as James Acton of the Carnegie Endowment for International Peace writes in a recent report, Rokkasho is likely to open because the surrounding area counts on it for economic development, whereas nuclear power plant reopenings, which are more controversial in their local communities, are less of a sure thing.

There is no reason to believe that Japan plans to use its extra plutonium for weapons, and the country cooperates closely with the International Atomic Energy Agency to ensure compliance with safeguards. Still, choosing to let the stockpile grow further could worsen regional tensions, especially with China, which may question Japan's intentions. The reprocessed plutonium buildup also sets a harmful international precedent, for example with respect to Iran's nuclear program. If Japan restarted more nuclear plants and decreased its plutonium stockpile, it could help ease concerns about its intentions and set a good example, helping to decrease global nuclear weapons risk.

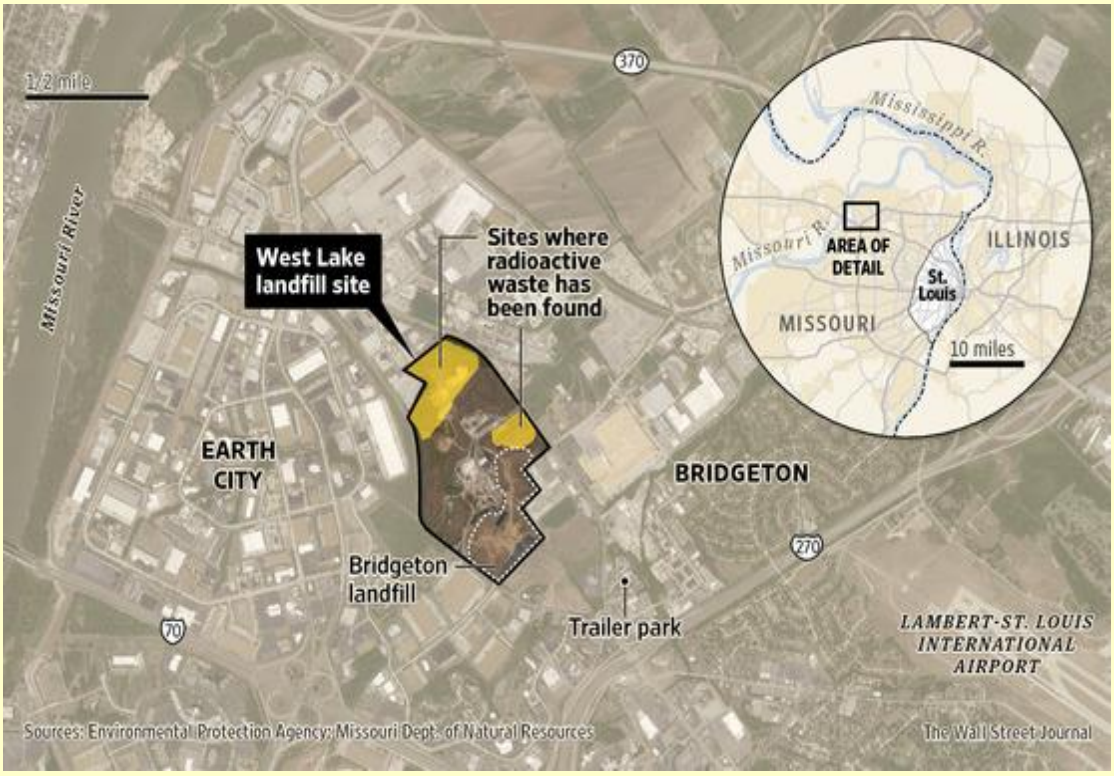
Of course, nuclear and coal are not the only electricity options. Other fossil fuels pose the same global warming and health problems as coal, albeit to a somewhat smaller degree. Renewables do not, but Japan has been slow to adopt them. Ultimately a full transition to renewables may be a good idea, but that will take time, and nuclear power plants can be restarted now. Bringing them back online would be the best current energy option for Japan and for the world.

***Seth Baum** is executive director of the Global Catastrophic Risk Institute, a nonprofit think tank that Baum co-founded in 2011. Baum's research focuses on risk, ethics, and policy questions about major threats to human civilization, including nuclear war, global warming, and emerging technologies.*

Residents of a St. Louis suburb worry about landfill containing nuclear waste

Source: http://www.homelandsecuritynewswire.com/dr20151029-residents-of-a-st-louis-suburb-worry-about-landfill-containing-nuclear-waste

Oct 29 – Residents of a St. Louis suburb are increasingly anxious over a potential nuclear threat buried in the ground. One landfill nearby contains nuclear waste, while in a second landfill, only 1,000 feet away, there is "hot spot" burning underground.



CBS This Morning reports that federal officials insist the "smoldering event" is contained, and not moving toward the nuclear waste in the first landfill.

The residents are not reassured, however, and on Monday hundreds of them demanded answers from the federal officials.

"You can't 100 percent guarantee that we're okay," said one resident.

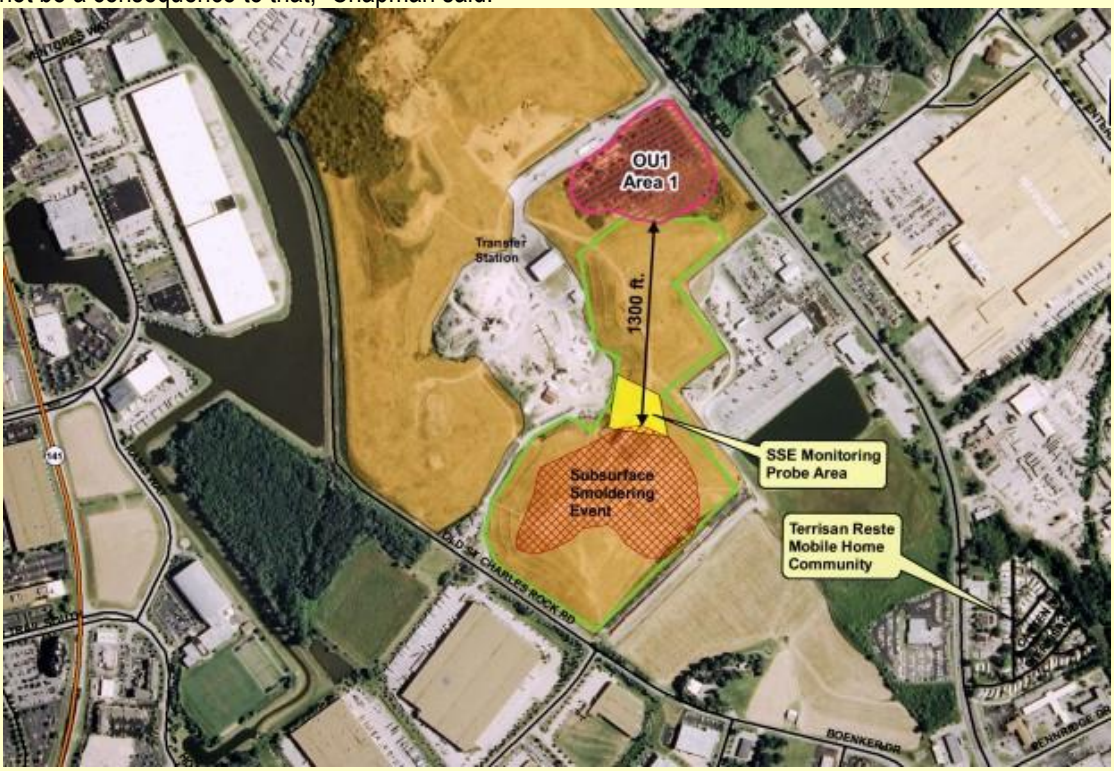
"We don't go outside, we don't open our windows," said another.

St. Louis' nuclear waste problems go back to the Second World War, when a local facility processed uranium for the U.S. first nuclear weapons. In 1990 one landfill was named a Superfund cleanup site, and it contains illegally disposed nuclear waste from the cold war era. The fire in the second landfill has been smoldering for five years.

The sites where the nuclear waste was stored have been cleaned, but low-level radiation has moved into neighborhoods.

"I don't know why they ignored it for so long, I really don't," Dawn Chapman, who lives less than two miles away from the landfills, told CBS. Chapman was among the founders of the activists group to educate her neighbors.

"I cannot believe that somebody and anybody in their right mind would think that you can leave the world's oldest nuclear weapon's waste sitting on the surface of a landfill for over forty years and there not be a consequence to that," Chapman said.



The state's attorney general is now suing the landfill's owner, Republic Services. The AG says the company has not handled the fire properly, and that state's experts warn that the underground fire could reach the nuclear waste in three to six months.

Both the company and the Environmental Protection Agency (EPA) reject these assessments. Republic has also spent millions of dollars over the years to contain the burn and control the foul odors.

"There's been a lot of concern and public comment on earlier decisions this agency made and it's time for us to give them a proposal," Mark Hague, an acting regional administrator for the EPA, told CBS.

The EPA is considering installing a barrier between the two landfills by the end of the year, but the residents insists that will not accept a barrier as an alternative to the removal of all the radioactive residue and extinguishing the burn.

There are other problems, though. Over the past weekend, a grass fire reached to within seventy-five yards of the radioactive waste, and the region sits near an earthquake fault line.

Explosion rocks nuclear power plant in Belgium

Source: https://www.rt.com/news/320381-belgium-nuclear-plant-explosion/

An explosion occurred overnight at a nuclear power plant in Doel, northern Belgium, local media reported, adding that the blast caused a fire. The exact damage from the incident remains unknown.

The blast happened around 11pm local time on Saturday. **The fire started in Reactor 1 of the plant, but was soon extinguished by personnel.**

The explosion didn't cause any threat to nature, Els De Clercq, spokeswoman from Belgian energy corporation Electrabel that runs the plant, told Het Laatste Nieuws. **There was no fuel present at the time of the incident as the reactor had been shut due to its expired operational license.**

Doel Nuclear Power Station, one of the two nuclear power plants in the country, is located near the town of Doel in east Flanders. The plant employs about 800 people.

According to the Nature journal and Columbia University in New York, the plant is in the most densely populated area of all nuclear power stations in the EU. **About 9 million people live within a radius of 75km of the station.**

22 Dec 2014 – An unidentified drone has been spotted hovering over a Belgian Nuclear power plant, prompting an investigation. The Doel nuclear plant has just been repaired and reopened after an incident considered to be sabotage caused millions in damages.

"We can confirm that the East Flanders prosecutor's office has opened an investigation into a drone flight over the Doel nuclear plant," a spokesman for the investigation told Belga news agency.

The plant's operator, GDF-Suez unit Electrabel disclosed the incident on Saturday. *"We will not provide further information for the time being,"* the spokesman added.

The facility in question is the Doel nuclear power plant which holds four of Belgium's seven reactors. It is located on a riverbank next to the North Sea, some 25 kilometres km from Antwerp.

The Doel 4 nuclear reactor was restarted Friday after an incident on August 5 halted it for months. The apparent sabotage saw 65,000 liters of oil escape in half an hour, leaving the rotating steam turbine without lubrication and causing serious damage. A €30 million ($37 mn) repair job was carried out in Germany to get the unit back on.

Did it fall from the Death Star? Mysterious black orb bearing an uncanny resemblance to Star Wars torture device is discovered in the middle of a Spanish field

Source: http://www.dailymail.co.uk/news/article-3305619/Did-fall-Death-Star-Mysterious-black-orb-bearing-uncanny-resemblance-Star-Wars-torture-device-discovered-middle-Spanish-field.html

Nov 05 – **A mysterious black orb has been discovered in the middle of a field after apparently falling from space.** Spanish goat farmers discovered the strange object, which bears a striking resemblance to the Star Wars torture device, the IT-O Interrogator, in Calasparra, Murcia. The men alerted the Civil Guard to investigate and the area was subsequently put under quarantine. Independent researchers have now attempted to provide an explanation for the orb.

The mysterious orb (left) bears a resemblance to the Star Wars torture device, the IT-O Interrogator (right)

The mystery object is not said to be dangerously radioactive or explosive but has been taken away for further analysis.
Local news site El Pais reported that researchers have said that the object may be a pressurised gas container, which fell to earth from space.

The Civil Guard confirmed that the object was an aerospace artefact and pointed to the possibility that it fell from a rocket or a satellite.

Meanwhile a local community manager has conducted his own research and deduced that the object appears to be a composite overwrapped pressure vessel, possibly from a space station.
The gas containers are created with extremely strong material that is designed to withstand re-entry into the earth's orbit.

A local community manager deduced that the object appears to be a composite overwrapped pressure vessel, possibly from a space station
A number of locals had other ideas however and the paper reported that some people had suggested that the orb had 'fallen from heaven'.
This is not the first time a mystery ball of this kind has fallen to earth from space with similar objects having been found in both Australia and Brazil.
The IT-O Interrogator is a droid that made an appearance in a number of Star Wars books and films.

Purposefully intimidating, the orb was used as a device to get information from prisoners using elaborate and scientific torture methods.

Souvenir: The mystery object is not said to be dangerously radioactive or explosive but has been taken away for further analysis

EDITOR'S COMMENT: I will not comment the stupid title of the article – usual in mass media in order to attract readers. But I will commend on the reaction plan as described in the photos of this article. A first responder in Level-A detects for radiation – fine! Although there something called EOD CBRN Robot that could do the job from a distance! A person from Civil Guard examines the object totally unprotected – not fine! And then the object is placed in a SUV to be taken home – no container used; not even a plastic. What if space microorganisms were present on the object? What if – so many ifs for an object they did not s… about its origin? You will say that this is not an orginary event? So what? Einstein's quota came back to my mind – you know, the one about space and stupidity!

How Al-Shabab Could Get Their Hands on a Nuclear Core

Source: http://www.defenseone.com/threats/2015/11/how-al-shabab-could-get-their-hands-nuclear-core/123403/

Nov 04 – **Last April, four al-Shabaab fighters killed 148 people at Garissa University in northeastern Kenya, just up the street from a major military installation.** While students fled, barefoot and in their nightclothes, the soldiers remained on standby, unsure how to respond, and elite police took hours to arrive. In September 2013, the Somalia-based Islamist militants attacked a mall in the heart of Nairobi, killing 67, most of them before any uniformed police or military showed up.

This does not sound like a country that should be getting a nuclear program, even a civilian one. And yet it is, getting an initial thumbs-up from the International Atomic Energy Agency in August.

Kenya says that it has no choice. By 2030, it will need 20,000 MW of electricity, and the current energy mix can't meet those needs. Droughts, getting longer and more frequent, will undermine hydropower plants, which provide more than 50% of the power today. Neighboring Tanzania said

earlier this month that it would have to temporarily turn off all its hydropower plants because of low water levels, and plans to reduce its dependence on hydro.

Meanwhile, geothermal energy will top out at a maximum of 10,000 MW—Kenya is unable to capture any more than that. Solar energy will remain part of the mix as well, but not at a scale that can meet the demand. "We have no option but to embrace nuclear early enough to avoid starting the process long after we have exhausted geothermal sources," said Joseph Njoroge, one of the country's top energy officials.

So what of the nightmare scenario—a terrorist group seizing control of a nuclear power plant and getting hold of its core? It has been quiet in much of Kenya since the attack on Garissa, but there is a sense here that al-Shabaab is not weaker—just laying low, possibly planning another major attack.

The South Africa-based Institute for Security Studies convened a conference in Nairobi in September on United Nations Resolution 1540, which bans non-state actors from getting their hands on nuclear, biological or chemical weapons. Speaking on the sidelines, Nicolas Kasprzyk, a non-proliferation expert at South Africa's Institute for Security Studies, is confident that Kenya can keep a nuclear facility safe. He thinks public perception, not actual safety, is the big hurdle.

"Clearly more needs to be done to fight this situation with al-Shabaab. How can you build trust in your nuclear program if you're perceived as not managing to contain the terror threat?" he said. But as proof that Kenya is up to the task, he pointed to its experience protecting medical research facilities with specimens that could easily be turned into biological weapons. There are two level-3 biosafety laboratories (which can handle all but the most lethal diseases) in the vicinity of Nairobi that have been kept secure—both from terrorists and from human error—for years now.

That being said, Kasprzyk pointed out that nowadays it's the private sector, not government research institutes, that has the most contact with dual-use goods—materials that could be used for peaceful or non-peaceful purposes. And where governments in the region often fall short is proper private-sector oversight, meaning materials might get siphoned off or stolen without government knowledge. Although Kenya has not yet said who will build the nuclear power plant, it's likely to be a private company.

"The two of them just don't have a dialogue on proliferation,"Kasprzyk says, referring to the government and private sector. "You can't exclude that could be diverted… you have a genuine risk," he said.

New, portable radiological detectors for frontline personnel

Source: http://www.homelandsecuritynewswire.com/dr20151113-new-portable-radiological-detectors-for-frontline-personnel

Nov 13 – Recently, DHS's Domestic Nuclear Detection Office (DNDO) awarded a multimillion dollar contract which will equip U.S. Coast Guard (USCG), U.S. Customs and Border Protection (CBP), and Transportation Security Administration (TSA) frontline personnel with a new capability to detect and interdict radiological or nuclear threats.

DNDO says that the award is for small, wearable radiation detector devices that passively monitor the environment and alert the user when nuclear or other radioactive

material is present. Known as the **Human Portable Tripwire** (HPT), this device has the capability to identify the source of radiation and allow personnel to take appropriate action. **The technology can also locate the source of the detected radiation and includes communication features** that allow the user easily to seek additional technical assistance from experts if needed. These devices are a critical tool for personnel who operate in the maritime environment, at land and sea ports of entry, and within the United States.

DNDO says that the Human Portable Tripwire award represents a successful collaboration between CBP, USCG, TSA, and DNDO to award one contract that meets the needs of multiple DHS components.

"This is also an example of the accomplishments we can achieve under the Unity of Effort initiative," DNDO notes.

DNDO worked closely with CBP, USCG, and TSA from the proposal evaluation stage, through the testing and evaluation, to deployment planning. "Such collaborative efforts strengthen our homeland security and increase the Department's ability to thwart potential radiological or nuclear threats," DNDO said.

Lawmakers Concerned over Threat of Dirty Bomb to US Ports

By Amanda Vicinanzo, Senior Editor

Source:

Nov 04 – **It's the stuff of nightmares and thrillers. Terrorists detonate a dirty bomb at a US port and the nation plummets into chaos as the radioactive material spreads across dozens of square miles, resulting in thousands of lost lives and billions of dollars as the nation struggles to recuperate in the wake of the attack.**

Although a dirty bomb attack on a US port would take a tremendous toll on the economic health and security of the nation, lawmakers have expressed concern the US is not doing enough to deter, detect and interdict potential security threats to the nation's ports.

With that in mind, the House Committee on Transportation and Infrastructure Subcommittee on Coast Guard and Maritime Transportation recently held a hearing to discuss the vulnerability of US ports to terrorist attacks using a dirty bomb, a type of radiological dispersal device (RDD) that combines conventional explosives such as dynamite with radioactive material like Cobalt 60.

Although terrorists have yet to launch a successful RDD attack on US soil, the threat is real and terrorists have shown an interest in RDDs. In his opening remarks before the hearing, Subcommittee Chairman Duncan Hunter (R-Calif.) said in early October the Associated Press reported on FBI and Eastern European authorities' efforts over the last five years to successfully interrupt four attempts by criminal gangs with suspected Russian ties to sell radioactive material to Middle Eastern extremists. And it's not the first time jihadists have attempted to obtain radiological materials.

"The successful disruption of the sale was a positive result," Hunter said. "However, the desire of our adversaries to obtain, at a minimum, materials for a dirty bomb, or even materials for a nuclear weapon are growing."

Al Qaeda publications show terrorists consider an RDD attack because of its devastating economic and psychological consequences.

In August, three men -- Dhiren Barot, Jose Padilla and Glendon Crawford -- were convicted for attempting to **develop and use an RDD in New York City, Chicago and elsewhere**, according to the testimony of Charles Potter, distinguished member of the technical staff at Sandia National Laboratories.

"Obtaining a clear picture of adversary planning is difficult, and it is it is prudent to assume that the necessary motive and intent exists," Potter said. "Our duty then is to ensure that credible scenarios leading to high-consequence RDD attacks are made as difficult as possible to our potential adversaries."

Current US efforts to protect ports from a dirty bomb attack

Customs and Border Protection (CBP) officials testified the agency currently employs a multi-layered approach to port security. CBP works closely with domestic and international partners to protect the nation's ports and waterways, according to Todd Owen, CBP Assistant Commissioner, Office of Field Operations.

Owen stated CBP's approach includes three layered elements "to improve supply chain integrity, promote economic viability, and increase resilience across the entire global supply chain system:"

Advance information and targeting. Obtaining information about cargo, vessels and persons involved early in the shipment process and using advanced targeting techniques to increase domain awareness and assess the risk of all components and factors in the supply chain.

Government and private sector collaboration. Enhancing our federal and private sector partnerships and collaborating with foreign governments to extend enforcement efforts outward to points earlier in the supply chain; and

Advanced detection equipment and technology. Maintaining robust inspection regimes at Ports of Entry, including the use of non-intrusive inspection equipment and radiation detection technologies.

Partnerships, in particular, are one of the most crucial elements of CBP's risk-based strategy for port security. For example, since 9/11, the Customs-Trade Partnership against Terrorism (C-TPAT) has been an important tool supporting the nation's efforts to secure the global supply chain while facilitating the secure and efficient flow of legitimate cargo.

Launched in November 2001, **C-TPAT** is a voluntary program in which CBP officials work with private companies to review the security of their supply chains and improve the security of their shipments to the United States. In return, C-TPAT partners receive various incentives, such as reduced scrutiny of their shipments.

Another international cargo security initiative used by CBP is the **Container Security Initiative** (CSI), which the agency established in 2002 with the sole purpose of preventing the use of maritime containerized cargo to transport a weapon of mass destruction (WMD) by ensuring all containers identified as potential risks for terrorism are inspected at foreign ports before they are placed on vessels destined for the United States.

"Each year, more than 11 million maritime containers arrive at our Nation's air and seaports," Owen said. "At our land borders, another 11 million

arrive by truck and 2.7 million by rail. CBP's targeting activities, in conjunction with programs like CSI and C-TPAT, increase CBP's awareness of what is inside those containers, and enhance our capability to assess whether it poses a risk to the American people."

"Working with our DHS, Federal, international, state, local, tribal and private industry partners, CBP's cargo security programs help to safeguard the nation's borders and ports from threats -- including those posed by radiological weapons," Owen continued.

Is US prepared for a dirty bomb attack?

If a dirty bomb ends up in the wrong hands, our country is at grave risk. Consequently, stopping dirty bombs before they reach our shores must be a priority. However, current US efforts are not up to the task of preventing a determined adversary from targeting a US port with a dirty bomb, according to the Dr. Stephen Flynn, director of the Center for Resilience Studies at Northeastern University.

According to Flynn, there is a real and present danger that containers will be used as modern-day Trojan horses. The reality is, no one really knows what is inside a container except those who are there when the container is packed, since CBP officials rely on the cargo manifest -- which can easily be falsified --for this information.

In 2012, CBP admitted there could be a serious vulnerability within the US in-bond cargo program regarding the contents, access and whereabouts of in-bond cargo shipments. Moreover, a 2013 Government Accountability Office (GAO) audit found CBP has not assessed the risk posed by foreign ports that ship cargo to the United States for its Container Security Initiative program since 2005.

More recently, a GAO audit determined CBP has not been accurately recording the disposition of high-risk maritime shipments, which may be creating vulnerabilities in the supply chain.

Given the inadequacy of current efforts to secure the global supply chain from point of origin, Flynn believes the US should switch its emphasis from policing US-bound cargo to working with US trade partners and the private sector to monitor and validate the flow of legitimate global cargo.

"Should a dirty bomb that originated overseas be set off in a US port, it would represent a major security breech in the global supply system that will result in US port closures," Flynn said. "This, in turn, will place the intermodal transportation system at risk of widespread economic disruption generating tens of billions of dollars in losses, and potentially endangering lives as the shipments of critical time-sensitive goods such as medical supplies and defense-related materials are interrupted."

Flynn added that, "Since the current US container security programs are inadequate for addressing these stakes, the way ahead must involve a far more vigorous effort by the US government to provide incentives for US trade partners and private sector participants to share the responsibility for closely monitoring and validating the international flows of legitimate cargo and to develop robust contingency plans managing security incidents."

Dr. James Giermanski, chairman of Powers International Inc., has expressed similar concerns to *Homeland Security Today* on multiple occasions. Giermanski believes current CBP efforts to secure the supply chain are merely "smoke and mirrors," since the agency does not use off-the-shelf state-of-the-art technology to ensure containers remain secure from point of origin to destination.

Giermanski advocates the use of in-container tracking mechanisms which actually identify the person at origin who physical verifies the cargo, seals the container and triggers global monitoring all the way to origin, including any access to the container at transshipment ports. These mechanisms provide an auditable record of actual people and their behavior along with the integrity of the container itself.

Concerns regarding RDD attacks are not limited to detection. Potter expressed deep concerns over current US efforts to recover from an attack. Currently, there is no single US standard for post-cleanup radiation levels, making it difficult to estimate the costs that would be directly associated with decontamination.

"The RDD risk is real and multi-faceted, and the US government has implemented a number of programs to increase the security of US radiological materials and increase the difficulty of illicit movement of these materials, resulting in a reduced likelihood of an RDD attack," Potter said. "However, there is still significant uncertainty in our

understanding of the costs that would accrue after such an event."

"The development of policies and technical capabilities for effective cleanup to allow for resumption of normal operations following an RDD attack would constitute an important element of the multi-dimensional, integrated solution for addressing the RDD threat," Potter concluded.

100 percent scanning of cargo at US ports

During the hearing, Rep. Janice Hahn (D-Calif.) said although ports are the "economic engine" of the country, in the wake of the 9/11 terrorist attacks more time, effort and money has been devoted to airports than to the protection of US ports.

"When people ask me what keeps me up at night? A dirty bomb at the Port of Los Angeles, or Long Beach," Hahn said. "Ships make 50,000 calls a year on our US ports. They carry 2 billion tons of freight, 134 million passengers -- they are incredibly important and one dirty bomb at Long Beach, Los Angeles would be disastrous."

Hahn also reiterated her call for 100 percent scanning of all cargo at US ports, noting that only 3 percent of the cargo shipped through US ports is scanned for contraband and dangerous materials, like explosive devices. Hahn recalled incidents in 2002 and 2003 where ABC News smuggled depleted uranium through the ports of New York and Long Beach and no one detected it.

As *Homeland Security Today* previously reported, Hahn introduced legislation last year that would require 100 percent scanning of cargo containers at domestic ports and would allow select ports to receive federal funding for advanced inspection technology to implement 100 percent scanning of shipping containers for radiological and nuclear material as well as other potentially dangerous material.

"I have said it once and I will say it again, we need 100 percent scanning at our ports," Hahn said at the hearing. "The risks are too high not to."

Congress has passed two pieces of legislation, the Security and Accountability For Every (SAFE) Port Act of 2006 and the Implementing Regulations of the 9/11 Commission Act of 2007 requiring 100 percent scanning of incoming cargo at US ports. However, the mandate has yet to be implemented. The Department of Homeland Security missed the 2012 deadline, as well as another in 2014, and continues to delay its implementation of the policy due to a purported lack of resources.

Hahn stated another one of the biggest reasons cited for not implementing 100 percent screening is that it would slow down the flow of commerce and impede the economy. However, the congresswoman believes there is technology available that would not disrupt the flow of commerce.

In the June/July 2015 issue of *Homeland Security Today*, for instance, Dr. Gene W. Ray, CEO of Decision Sciences International Corporation (DSIC), indicated the 100 percent screening mandate can be met with the right technology. For example, DSIC has harnessed the natural power of muons -- subatomic particles similar to electrons created by cosmic rays entering the Earth's atmosphere -- with its **multiple mode passive detection system** (MMPDS) for detecting materials in shipping containers and other types of conveyances.

The MMPDS technology can detect shielded and unshielded nuclear material, as well as explosives and contraband, such as tobacco. MMPDS, unlike an X-ray, can see into a dense object like lead to determine whether there is a threat. Moreover, the more muons going through, the better the system will be able to detect a potential threat.

Dr. Gregory Canavan, a senior fellow at Los Alamos National Laboratories, told the subcommittee technologies could be implemented that would not impede the flow of commerce. He testified that that compact, fast neutron detection systems can give confident detection of nuclear materials with low false alarms rates.

"Compact fast neutron inspection provides high-confidence detection of disseminated nuclear designs, materials and technologies on the time scale on which they could be integrated to take advantage of the large number of containers entering US ports," Canavan said. "They could be deployed on ships, ports, or at sea to support first line defense of the US against nuclear weapons in a manner consistent with the role of the Coast Guard."

The Greatest Terrorist Threat

By Sam Nunn, Richard Lugar and Des Browne
Source: http://www.politico.com/magazine/story/2015/11/the-greatest-terrorist-threat-213370#ixzz3rpv85QNo

Nov 17 – Let there be no doubt: If the radical jihadists responsible for the latest assault on innocents in Paris get their hands on weapons of mass destruction, they will not hesitate to use them. There is no limit to the horrible acts terrorists will carry out in pursuit of their ideological agenda. The best way to stop a WMD attack is to prevent terrorists from obtaining nuclear materials in the first place.

If terrorists were able to detonate a crude nuclear weapon built with materials they stole or bought on the black market, the catastrophic consequences could easily include the deaths of tens or hundreds of thousands of people, the wide-scale destruction of property, the disruption of global commerce and restrictions on civil liberties worldwide. Citizens and leaders alike would be left to ask: "What could we have done, and what should we have done, to prevent it?"

The good news is that leaders and governments have been focused on this concern for a number of years and can point to progress in better securing and removing some of the world's most dangerous nuclear material—the highly enriched uranium and plutonium that could be used to build a bomb—scattered across the globe. Thanks to work that began in the early 1990s and has intensified through biennial Nuclear Security Summits since 2010, we've reduced the number of countries possessing nuclear materials from 52 in 1992 to 24 today.

Yet as leaders prepare for the Nuclear Security Summit in Washington, D.C., in March 2016, there is still ample cause for concern. Today, more than 1,800 metric tons of weapons-usable materials remain stored in countries around the world, some of it still too poorly secured and vulnerable to theft. A recent report on a sting in southeast Europe exposed another chilling reality: a black market in nuclear materials. Compounding the threat is the fact that it doesn't take much material to build a bomb and the technical know-how needed to do it is more accessible than ever.

We also know that, despite leaders' efforts, there is still no effective global system in place for how all weapons-usable materials should be secured. Implementation of existing international guidelines remains far from universal, and no mechanism exists for holding countries accountable for lax security at nuclear facilities. **Moreover, even those mechanisms that do exist apply almost exclusively to a small fraction of all weapons-usable nuclear materials—the 17 percent used for peaceful, civilian applications. The remaining 83 percent are commonly characterized as "military materials" and are therefore outside the scope of current international security standards and mechanisms.**

As recent security breaches at military facilities in the United States and elsewhere have made clear, lax regulation on military materials is incredibly dangerous. Just consider the case of the 82-year-old nun and her fellow peace activists who broke into the Y-12 National Security Complex in Oak Ridge, Tennessee, in 2012. Known as the "nuclear Fort Knox," the Y-12 facility is operated by the Department of Energy and houses thousands of kilograms of highly enriched uranium. These activists spent nearly 1½ hours on the facility compound before a single guard noticed and arrested them for trespassing. Next time the intruders might not be so harmless.

Radiological materials, such as those used in medical equipment and scientific research, pose another largely unaddressed threat. These are materials that could be used to build a "dirty bomb" that would not kill thousands but could spread radioactive materials and contaminate

and deny access to major portions of one of the world's great cities or ports, causing billions of dollars in damage and sowing terror. Already, there are claims that Islamic State extremists may have stolen enough material to build one of these bombs.

As the 2016 Nuclear Security Summit approaches, we applaud leaders for engaging on the threat and for taking the steps they have already taken to remove and secure vulnerable materials, but we have a long way to go.

In addition to minimizing and eliminating these dangerous materials and the number of facilities where they are located, leaders must work to build a strengthened global security system. The system should cover all nuclear materials, including "military materials," and apply international standards, best practices and measures that build confidence in the effectiveness of each state's materials security. States also should work to:

- Secure all nuclear materials and facilities to the highest standards, including screening personnel with access to sensitive materials and facilities; and strengthen tools to prevent and detect the trafficking of nuclear materials across borders.
- Ensure accountability through independent oversight and build a strong security culture that includes peer reviews, best practice exchanges and realistic security exercises and assessments.
- Strengthen international cooperation on nuclear security, which should include reviving cooperation between the United States and Russia and enhancing intelligence and law enforcement cooperation.

Leaders also must do more to counter the dirty bomb threat. Last year, 23 countries at the Nuclear Security Summit agreed to secure their most dangerous radiological materials. Next March, additional countries should join the pledge. In addition, hospitals should replace blood irradiators that use the most dangerous material, cesium-137, with now available alternative technologies that achieve equivalent medical outcomes.

Now, as we mourn the victims of the Paris attacks and as France and its allies avenge their loss, we call on world leaders to dramatically step up efforts to tighten security around the dangerous materials needed to build weapons of mass destruction and disruption. In the face of escalating threats, leaders have an obligation to their citizens, to their neighbors, and to the wider global community to do all that they can to prevent catastrophe.

__Sam Nunn__ is a former U.S. senator.
__Richard Lugar__ is a former U.S. senator.
__Des Browne__ is a former UK secretary of state for defence. All three serve on the Board of Directors of the Nuclear Threat Initiative.

Beyond Paris - A Growing Terrorist Threat

By Richard Schoeberl

Source: http://www.domesticpreparedness.com/Commentary/Viewpoint/Beyond_Paris_-_A_Growing_Terrorist_Threat/

Paris is the most recent reminder of the barbaric acts of brutality and terrorism committed by the Islamic State. Although this extremist terror organization has committed despicable acts – such as crucifixions, beheadings, live burnings, and bombings – the threat of its brutality is expanding beyond Europe, with even deadlier consequences.

Nov 18 – The fear of terrorist attacks grew after three teams of terrorists staged synchronized attacks at separate locations throughout Paris, France, on 13 November 2015 – including a concert hall, the Stade de France, and multiple restaurants. At least 129 people were killed in the attacks, and 352 people were wounded – 99 of them seriously. The Islamic State has claimed responsibility for these attacks, as it did for the killing of 224 people when a Russian airliner crashed in Sinai on 31 October 2015. To complicate matters, intelligence suggests that the Islamic State has the means to acquire a chemical, biological, radiological, or nuclear (CBRN) weapon.

Implications of the Paris Attack

There must be a unilateral strategy to combat the terrorist threat, both domestically and abroad. As long as the Islamic State continues to maintain a haven in which to operate, train, and spread radical ideology, the world will continue to face acts of terror. On Monday, 16 November 2015, less than 48 hours after gunmen and suicide bombers synchronized attacks across the city of Paris, U.S. President Barack Obama defended his strategy for combating the Islamic State. During a news conference at the G20 Summit in Turkey, Obama stated that sending large numbers of ground troops to Syria and Iraq would be a "mistake." Conversely, the only way to combat this threat is through a sustainable effort that is relentless to diminish the popularity that has ultimately led to the success of the Islamic State.

Most recently, a video purportedly released by the Islamic State shows a fighter standing with his followers, praising the Paris attacks, and threatening the United States, "As we struck France in its stronghold, Paris, we will strike America in its own stronghold in Washington." This new video warns of lethal consequences should the United States, or any country, partner with France against the Islamic State. The video further warned European nations not to block the terrorists' efforts across Syria and Iraq. This new information suggests a major shift in the terrorist group's global strategy. Once content with regional dominance, the Islamic State is now pushing to expand its control throughout the European communities and elsewhere.

The complexity of the Paris attacks suggests extensive planning and preparation with direction from the Islamic State's central leadership. Adding to concern for national security in the United States is the Syrian refugee crisis. European officials say that professional terrorists are joining refugee travels in attempts to enter Europe and elsewhere. One of the suicide bombers at the Stade de France was in possession of a fake Syrian passport and arrived among the refugees on the Greek island of Leros on 3 October 2015. This is a concern because, in September 2015, the United States agreed to take 15,000 Syrian refugees, with approximately 85,000 total refugees expected by the end of 2016. The rise of the Islamic State, and its leaders' appeals for supporters to carry out attacks around the world, has prompted a sharper sense of caution both domestically and abroad.

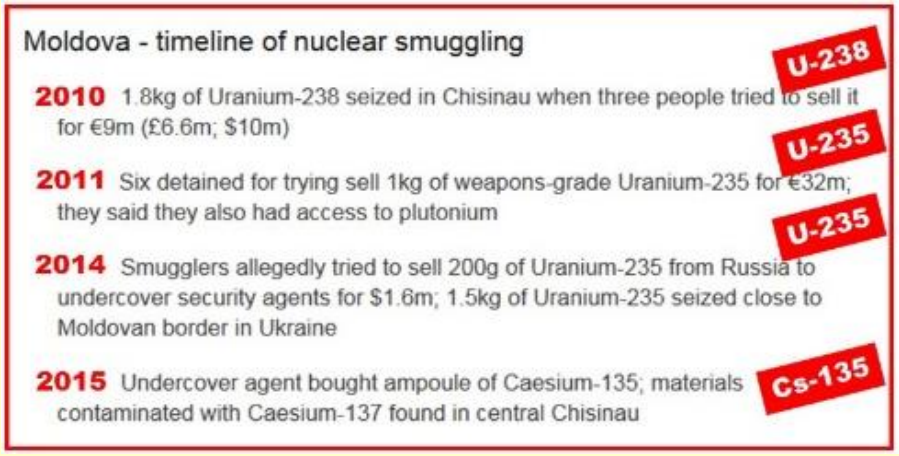
The Islamic State has an external agenda and is determined to carry out similar attacks outside of the region it has so quickly dominated. This is not an isolated event, and the Islamic State likely has additional attacks in the queue. This was a carefully planned attack in Paris over the course of several months, with trained operatives in place equipped with weapons such as explosives and suicide belts. The Islamic State has found more utility in trying to recruit and motivate sympathizers in the United States online from abroad. The FBI stated that "hundreds, maybe thousands" of U.S. residents currently follow the Islamic State online. In the past year, at least 49 people in the United States have been charged with terrorist-related crimes.

Many Buyers & Sellers

There is sufficient evidence and intelligence to conclude that an array of terrorist organizations representing various backgrounds and posturing different ideologies have attempted to acquire and have definitely considered the use of CBRN weapons. Although al-Qaida leaders have been outspoken about attempting to acquire or produce weapons of mass destruction (WMDs) for well over a decade, they have had no success in achieving these goals.

In 1998, then al-Qaida leader Osama bin Laden acknowledged that the acquisition and use of WMDs was his Islamic duty. During his leadership, bin Laden urged his top commanders to make efforts to acquire and develop nuclear and biochemical WMDs. However, more concerning is the looming fear that there are active sellers currently seeking Islamic extremist buyers. For example, **in Moldova, a former Soviet state in Eastern Europe, 68 percent of the population is low-income or living in poverty, which raises concern about a possible correlation between poverty and ongoing organized criminal activity.** Moldovan officials, working in conjunction with the Federal Bureau of Investigation, have thwarted at least four attempts in the past five years by suspected Russian organized crime groups to sell radioactive material to Middle Eastern extremists.

The latest attempt to illegally sell CBRN weapons occurred in February 2015, when a Russian smuggler offered a large cache of **cesium 135** to what he thought was a buyer from the Islamic State. According to the investigation, the smuggler offered a supply of cesium 135 in trade for 2.5 million Euros. Fortunately, the buyer was an informant rather than a member of the terrorist organization. According to the Moldovan investigators, most of the criminal organizations in Moldova have connections to the Russian KGB's (former Russian secret police and intelligence agency) successor agency, the FSB (Russia's Federal Security Service), and are flooding the country's black market with nuclear materials.



Dirty Bombs – Blueprints & Isotopes

In 2011, a Russian organized crime group attempted to arrange the sale of bomb-grade uranium (U-235) along with a set **of blueprints for a "dirty bomb"** to an unknown man from Sudan. The isotope U-235 is significant because, under various conditions, it can easily be split to yield a lot of energy. Therefore, it is said to be "fissile" – capable of splitting and releasing enormous amounts of energy – according to the World Nuclear Association. The properties of uranium are important for nuclear weapons and nuclear power because of their ability to fission and create the successful chain reaction that causes a nuclear explosion.

According to the Associated Press, in October 2015, authorities in Moldova blame the increase in black market sales of radioactive material on the breakdown in collaboration between Russia and the United States. Authorities claim that smugglers are finding new means to move Russia's vast unaccounted radioactive materials that have leaked into the black market, and these materials are controlled by organized crime. About 140 cases of missing or unauthorized use of nuclear and radioactive material were reported to the United Nations Atomic Energy Commission in 2013.

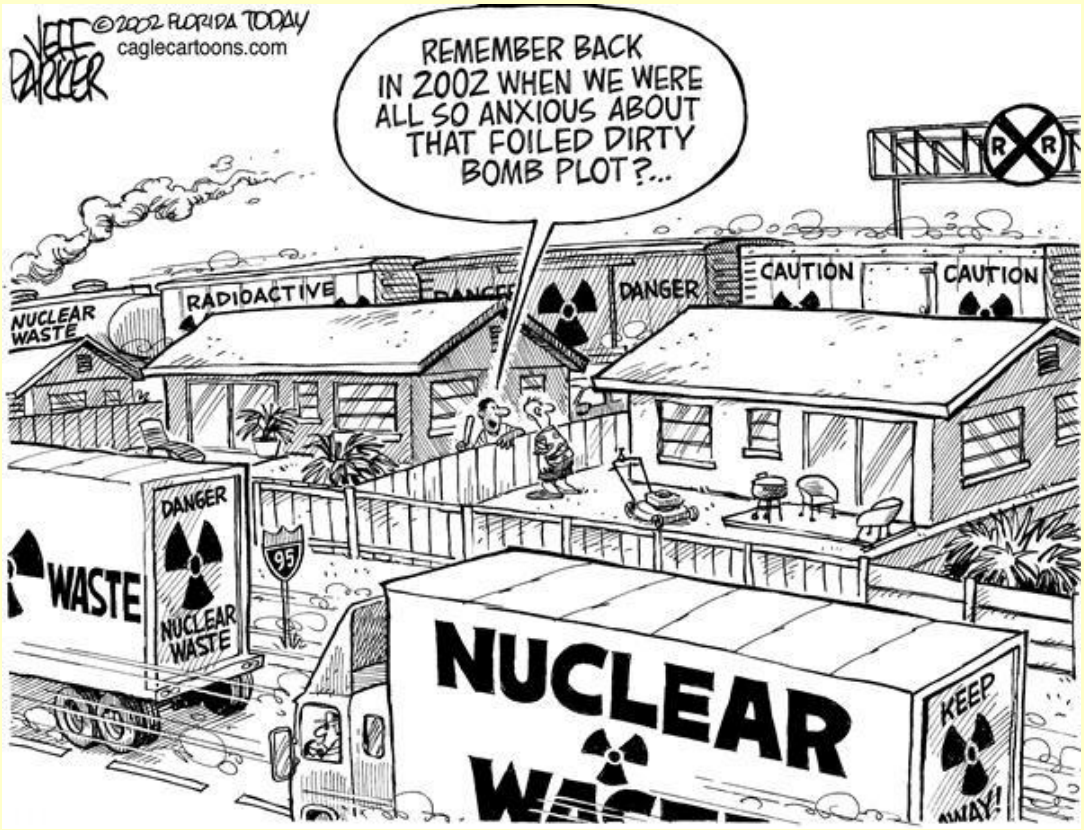
An official source from the U.S. Department of Energy told ABC News in 2005 that there is simply no way to calculate the amount of material that is missing in Russia. Neither the Russian nor Soviet government had ever used an accurate inventory system to track the quantity of nuclear material produced and the locations where it would be used. The stark reality is that, with a great deal of unaccounted materials after the collapse of the former USSR, coupled with eager buyers manifested by profiteers in the black market, an actual attack is simply a game of statistics.

Closing Statistically Significant International Gaps

Fortunately, the manufacturing of CBRN weapons requires access to bodies of scientific knowledge that, for the most part, have been the invention of western science and research. Although much of this knowledge is now published and available on the Internet, it still requires a certain level of access to training and research institutions to be made most effective. In order for the Islamic State to pursue a rigorous CBRN weapons program, the terrorist group would have to devote substantial resources to the acquisition, production, and, in some cases, tests of the weapon.

The sale of cesium is a concern for anyone in the international community because of the possibility of it being used to create a "Dirty Bomb" and expose large populations to the effects of radiation exposure – burns, acute radiation sickness, cancer, or even death. If the Islamic State were able to procure and weaponize the cesium, it could prove problematic for the ongoing conflict. Without a solid strategy for combating the Islamic State, the threat of Islamic extremists attempting to acquire CBRN weapons continues to be a challenge. Coupled with the fact that opportunists are actively seeking extremist buyers, the statistics game becomes increasingly more difficult with each passing day.

Richard Schoeberl *has over 20 years of security and law enforcement experience, including the Federal Bureau of Investigation (FBI) and the Central Intelligence Agency's National Counterterrorism Center (NCTC). He has served at a variety of positions throughout his career ranging from supervisory special agent at the FBI's headquarters in Washington, D.C., to acting unit chief of the International Terrorism Operations Section at the NCTC's headquarters in Langley, Virginia. Before his managerial duties at these organizations, he worked as a special agent investigating violent crime, international terrorism, terrorist financing, cyberterrorism, and organized drugs. He also was assigned numerous collateral duties during his FBI tour – for example, as a certified instructor and member of the agency's SWAT program. In addition to the FBI and NCTC, he is an author and has served as a media contributor for Fox News, CNN, PBS, NPR, Al-Jazeera Television, Al Arabiva Television, Al Hurra, and Sky News in Europe. Additionally, he has authored numerous articles on terrorism and security.*



Dynasafe Provides Explosive Detection Dog Teams Across All Airports in Afghanistan

Source: http://www.hstoday.us/single-article/dynasafe-provides-explosive-detection-dog-teams-across-all-airports-in-afghanistan/00055624746c1431678a13dd6fcffd07.html

Dynasafe announced it has been awarded a contract to provide Explosive and Narcotics Detection Dog Teams, as part of the general security package across all Afghan airports. This contract follows other significant Dynasafe contracts in countries such as Syria, South Sudan and Mali.

In Syria, Dynasafe dog teams continue to provide critical protection against Improvised Explosive Devices (IEDs) and vehicle bombs to the UN mission in Damascus. In Mali, another UN mission is similarly protected against rebel or terrorist attacks by Dynasafe dog teams. In South Sudan, the dog teams provide assistance to the humanitarian efforts in the country, supporting the security provision in the main UN camps.

Dynasafe has more than 12 years of experience in providing high quality search, detection and patrol dogs. The dogs are trained at a dedicated training facility, Dynasafe Canine Services, located in Pretoria, South Africa. On completion of their training, the dog teams will be deployed globally in the efforts to protect people and infrastructure from the threats of terrorism and conflict.

Adam Ainsworth, managing director of Dynasafe MineTech Limited said, "There is an increasing interest in our dog protection services and we have made further investments to the Dynasafe Canine Service facility to meet this growing demand. We look forward to providing long term security to those living in hazardous and high threat areas and continue to contribute to making the world a safer place."

FLIR Releases New Desktop Trace Detector

Source:http://www.hstoday.us/single-article/flir-releases-new-desktop-trace-detector/1903d930024438a869db434842a71139.html

Oct 15 – FLIR Systems, Inc is showcasing its latest addition to the Griffin 800-series desktop chemical trace detector product line at AUSA in Washington, DC this week.

The range is used by security officials to screen personal belongings, parcels, cargo, skin, vehicles and other surfaces for explosives and narcotics threats.

Launched on October 12, the new Griffin 844 has been designed to deliver a significantly lower false alarm rate than other offerings, and to provide expandability to address future threats without impacting sensitivity.

The Griffin 844 performs dual-mode detection for a range of current threats, including military, commercial, and home-made explosives, as well as commonly abused narcotics and synthetic drugs. FLIR's expandable library allows new threats to be added to the library without impacting sensitivity or false alarm rates. FLIR offers free updates to its Griffin library as they become available, providing customers with a future-proof solution that addresses emerging threats.

Built around FLIR's own mass spectrometry technology, the company said the Griffin 844 provides much higher resolution compared to existing ion mobility spectrometry technology, resulting in improved chemical selectivity. As a result, the Griffin 844 can yield significantly lower false alarm rates, providing confidence to security officers that only true threats are detected.

The Griffin 844 includes FLIR's menu-based GSS Touch

application, which is designed to streamline checkpoint operations. The Griffin 844's system design has been developed for fast and reliable clear-down that prevents lengthy bake-outs and minimizes maintenance to maximize operational availability. It uses a non-radioactive ionization source to eliminate associated costs and logistics.

FLIR is a supplier to the Department of Homeland Security and Department of Defense (DoD). Contract awards in 2015 include a second full-rate production order under a five-year indefinite delivery, indefinite quantity contract from the DoD to support the Nuclear, Biological and Chemical Dismounted Reconnaissance Sets, Kits and Outfits (DR SKO) program. The contract is for FLIR's integrated chemical, biological, radiological, nuclear, and explosives threat response system and related spares and services. The follow-on order is for systems totaling $51.1 million.

FLIR also received a production order totaling $19.5 million for its Mobile Surveillance Capabilities systems, the second option exercised for the procurement of additional units under its five-year firm-fixed price contract with Customs and Border Protection.

FLIR's MSC system is an integrated mobile surveillance and detection vehicle which features FLIR's TacFLIR 380HD long-range stabilized multi-sensor system and a long-range radar integrated into a vehicle-mounted surveillance tower.

Bomb threats force evacuations of Quebec schools

Source: http://www.cbc.ca/news/canada/montreal/quebec-schools-closed-over-security-concerns-bomb-threat-1.3301383

Nov 03 – **On Tuesday morning, upwards of 40 schools in the province and in the Ottawa region were evacuated, closed or searched after receiving a threatening email from an anonymous mailer.**

"Frankly, the people responsible for this tactic, whatever the nature of it is — and of course, we will allow the investigation to take its course — they have to know that they will be prosecuted, and that the investigation will be rigorous, if we are successful in identifying them," Couillard told reporters Tuesday at the National Assembly. "It's unacceptable. It's condemnable… Words escape me. It's criminal."

Meanwhile, schools across Montreal are trying to reassure worried parents, teachers and students that they are working with police concerning the bomb threats sent to schools.

Of the province's 48 CEGEPS (pre-university colleges), 20 received threats and five were evacuated, according to the Federation of CEGEPS. The schools that were evacuated are the cégeps in Drummondville, Lanaudière (Assomption

campus), Sept-Îles, Saint-Hyacinthe and Heritage.
Dawson College and John Abbott College were both searched by Montreal police as a precautionary measure.
Schools across the province and in the greater Montreal region were searched and in some cases, evacuated, as well.

Police investigations underway
Montreal police continue to search some local schools and CEGEPS, but no evacuations have taken place.
Both Montreal police and Quebec provincial police have launched investigations into the threats. Montreal police will meet with principals of schools that have been targeted or searched.
Interim Quebec Security Minister Pierre Moreau said the note cited anger at teachers' unions and quality of education as the main motivations for the threats.
"The nature of the email is a threat that bombs would be placed in schools, CEGEPS and some school buses as well because they are opposed to the way the teachers in Quebec and Ontario are dealing with the students," said Moreau.
Quebec provincial police have not said whether the threat is credible.
"Since this morning several schools in the province of Quebec received bomb threats, so the Sûreté du Québec takes these events very seriously," said provincial police Sgt. Mélanie Dumaresq.
"We took all possible actions to protect the population and make sure the students and teachers are safe."
Rodrigue Vigneault, president of Commission scolaire du Fer school board in Sept-Îles where 15 schools were affected, told CBC that all students were moved to a safe place.
"We received an email this morning. Only one school was named in that email but we don't take any chances and all the schools are closed," Vigneault said.

Montreal schools searched
Montreal police Const. Jean-Pierre Brabant said officers visited schools in Rivière-des-Prairies, Beaconsfield, Dorval and the Montreal borough of St-Laurent after the schools reported receiving threats.
Lester B. Pearson School Board chairwoman Suanne Stein Day did confirm that the board received a bomb threat note.
The English Montreal School Board has not been affected.
The two largest French-language school boards on the Island of Montreal have confirmed that schools are not being evacuated.
The Commission scolaire Marguerite Bourgeoys said it is

collaborating with Montreal police after receiving a note. It would not confirm whether police searched any of its schools, but said schools are not evacuated.

The Commission scolaire de Montréal has put an update on its website stating it has not received a threatening note, and it is following the situation closely.

What More Could Unmanned Systems Do: Underwater Mine-detection

Source: http://i-hls.com/2015/11/what-more-could-unmanned-systems-do-underwater-mine-detection/

Nov 03 – Singapore's Microfine Materials Technologies has won a defense prize for collaborating with DSO National Laboratories to design and build an unmanned underwater vessel that can detect mines in shallow water.

The annual Ministry of Defence (Mindef) event was held Friday to honour the defence research and engineering at The Chevrons club in Western region of Singapore, Straits Times reported Friday.

The main feature of M400 Autonomous Underwater Vehicle is its special sensor that will allow sailors to spot targets faster, will allow the navy to hunt down sea mines without putting sailors at risk.

The remote vehicle will be operational in two years. "Operated remotely by four people, the 600kg vessel will be able to match, if not surpass, the capabilities of the existing Mine Countermeasure Vessel, which is manned by 20 people," said Goh Ing Nam, DSO's Sensors Division programme director.

The vehicle will allow the navy to hunt down sea mines keeping sailors from risk.

"We have been tapping the innovativeness, agility and efficiency of smaller companies to complement what we can get from larger research labs and companies in our R&D efforts," said Mindef's chief defence scientist Quek Tong Boon, who believes more firms will be stepping ahead to partner the DSO.

"SMEs will be able to provide solutions for the armed forces, today's technologies, such as sensors and robotics, have dual purposes in the military and civilian world," said Mr Tong Boon.

Defence Minister Ng Eng Hen also gave out the top prizes to four people and another team for breakthroughs in their fields of research.

Paying tribute to the defence researchers and engineers, Dr Ng said, Singapore will continue to invest significantly to maintain, if not grow, the talent pool.

ISIS Posts Photo of Bomb That Brought Down Russian Plane

Source: http://silveristhenew.com/2015/11/18/isis-posts-photo-of-bomb-that-brought-down-russian-plane/

Nov 18 – Moments ago, ISIS released the 12th issue of its magazine profiled here previously, which had a cover page with a clear enough title: "**Just Terror**"

But while it has the usual content full of pro-Jihad propaganda, some 66 pages of it, as well as numerous images to commemorate the martyrs for the ISIS cause, what was most stunning about this edition was ISIS admission of how it brought down the Russian airplane above Egypt's Sinai peninsula, which as even Russia admitted yesterday, was the result of an ISIS bomb.

On page 3, we find the following two photos: one shows what Dabiq alleges are passports belonging to the "dead crusaders obtained by mujahidin"…

EXCLUSIVE - Image of the IED used to bring down the Russian airliner

… and more troubling, is the image of the IED used to bring down the Russian airliner**: a bomb concealed in a can of Gold beer.**

This is what the foreword to the magazine said. Notable is that ISIS says it had originally planned to bring down a plane "belonging to a nation in the American-led alliance" but changed its mind to blow up the Russian plane instead.

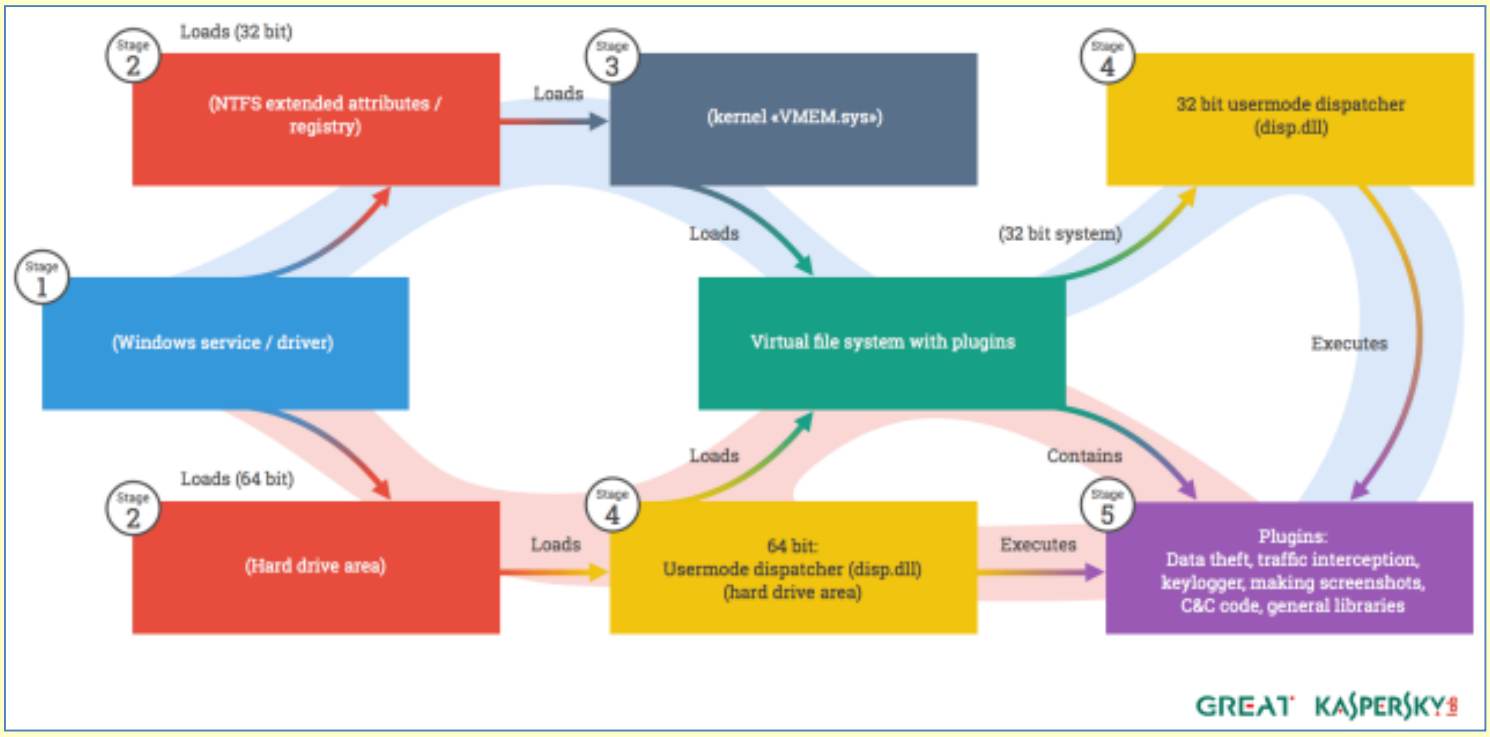

EXCLUSIVE - Passports belonging to dead crusaders obtained by the mujāhidīn

On "30 September 2015," after years of supporting the Nusayr in the war against the Muslims of Sham, Russia decided to participate directly with its own air force in the war. **It was a rash decision of arrogance from Russia, as if it held that its wars against the Muslims of al-Qawqz were not enough offence.** And so **after having discovered a way to compromise the security at the Sharm el-Sheikh International Airport and resolving to bring down a plane belonging to a nation in the American-led Western coalition against the Islamic State, the target was changed to a Russian plane. A bomb was smuggled onto the airplane, leading to the deaths of 219 Russians and 5 other crusaders only a month after Russia's thoughtless decision.**

For those curious about the authenticity of the photo, or to learn more about ISIS' propaganda, the magazine can be found here and is reposted below.

Top German official infected by highly advanced spy trojan with NSA ties

Source:



A diagram of the Regin platform.

Oct 26 – German Chancellor Angela Merkel may not be the only high-ranking leader from that country to be spied on by the National Security Agency. According to a report published over the weekend, German authorities are investigating whether the head of the German Federal Chancellery unit had his laptop infected with Regin, a highly sophisticated suite of malware programs that has been linked to the NSA and its British counterpart, the Government Communications Headquarters.

As Ars reported almost 12 months ago, Regin is among the most advanced pieces of malware ever discovered, with dozens of modules that can be used to customize attacks on targets in the telecommunications, hospitality, energy, airline, and research industries. Its technical DNA bears some resemblance to previously discovered state-sponsored malware, including the espionage trojans known as Flame and Duqu, as well as Stuxnet, the computer worm and trojan that the US and Israel reportedly unleashed to disrupt Iran's nuclear program.

According to research published last year by security firm Kaspersky Lab, Regin was used to infect more than 100 targets and has been active since 2008. Kaspersky Lab researchers went on to say that the targets included Belgacom, the partly state-owned Belgian telecom, and Jean-Jacques Quisquater, a prominent Belgian cryptographer. Documents leaked by former NSA subcontractor Edward Snowden have further linked Regin to the NSA, specifically to an NSA attack tool dubbed QWERTY. According to German magazine *Der Spiegel,* QWERTY is a keylogging plugin that's part of a much larger framework described in Snowden-leaked documents as WARRIORPRIDE. The takeaway is that Regin and WARRIORPRIDE are the same thing.

Kaspersky's investigation in 2014 into Regin is what led the researchers to first come upon The Equation Group, the name Kaspersky has given to a hacker group with NSA ties that operated clandestinely for 14 years before being discovered. The Equation Group is arguably the most sophisticated

team of hackers ever to come to light. Its list of almost superhuman technical feats include infecting the firmware of targets' hard drives using two zero-day vulnerabilities later folded into Stuxnet and the ability to use Web redirects to target iPhone users.

Over the weekend, *Der Spiegel* reported that Regin had been discovered infecting the laptop computer of a head of the Unit of the Federal Chancellery. The Federal Chancellery is the federal agency that serves the office of the Chancellor. The discovery comes after separate documents provided by Snowden in 2013 showed NSA agents eavesdropping on cell phone conversations of Merkel. Prosecutors in Germany investigated the claim but dropped the probe in June, citing insufficient evidence.

The Federal Prosecutor's Office has initiated an investigation into the latest discovery. So far, German officials have provided no timetable for the probe. Revelations that the NSA tapped Merkel's cell phone badly strained German-US relations. The latest discovery, that Germany was further targeted by a sophisticated espionage malware with NSA ties, isn't likely to help the two countries mend that rift.

Why the private sector is poaching cyber security experts from the public sector

By Simon Kouttis

Source: http://www.computing.co.uk/ctg/opinion/2431744/why-the-private-sector-is-poaching-cyber-security-experts-from-the-public-sector

Oct 23 – Recent high profile data breaches including Sony Pictures, Ashley Madison, and JP Morgan, which led to huge financial loss, claimed the heads of senior executives, damaged the public standing of these companies, and has ultimately elevated cyber security to the top of the boardroom agenda.

The result is an increased demand for cyber security expertise, which is in short supply. Part of this can be attributed to a lack of STEM skills nationwide: while these courses are well-funded (and more students are enrolling every year), universities are still not producing enough business-ready graduates to satisfy the rapidly expanding demand for cyber security skills. Longer term, governments and schools should do more to approach this problem from Key Stage through to college and A-Level. To treat STEM - and computer science in particular - as a priority subject from an early stage is imperative.

In the interim, however, companies are looking at industry to find the skills they need, but this takes time. And with so many companies competing for the same candidates, this can be difficult and expensive. In the immediate future, and until it is built into the curriculum, companies must look elsewhere to find the candidates they need.

Public sector poaching

Over the last year, we have seen a large number of candidates making the move from public sector to private. High-profile "defections" include Andy Archibald of the National Cyber Crime Unit, who previously spent 31 years in law enforcement.

What makes these candidates so suitable? Why are cyber analysts from the public sector being hired for private sector cyber security roles?

Unique skillsets

Hackers are becoming more sophisticated, which means companies are having to respond to stay one step ahead. They are now looking to build a more robust, mult-layered security capability, which consists of an incident response function complete with analytics and threat intelligence.

The public sector is a hotbed for developing cyber security skills. It has always invested heavily in training and development; there is a structured career progression so in a very short period of time it produces very highly skilled cyber security professionals. Such skills are nurtured through experience and military personnel are trained on the tools and techniques, which are universally transferable in industry.

So while military personnel may lack corporate experience, they have a very solid foundation and an education that is unparalleled in conventional routes. This makes them very attractive targets for private

companies looking for the latest cyber security talent. Not to mention the fact it is much more costly for a bank to poach from their competition.

How to attract public sector personnel

Salaries in the public sector are not comparable to what's on offer in the private sector, which is naturally a big draw for those looking to make the move. An analyst in the public sector, for example, will typically earn £35,000, but in the private sector the same position will command twice that. But it is not just money that motivates public service personnel. The private sector is investing heavily in the most cutting-edge technology and techniques; they offer a diverse, interesting office environment; and a much-improved work-life balance.

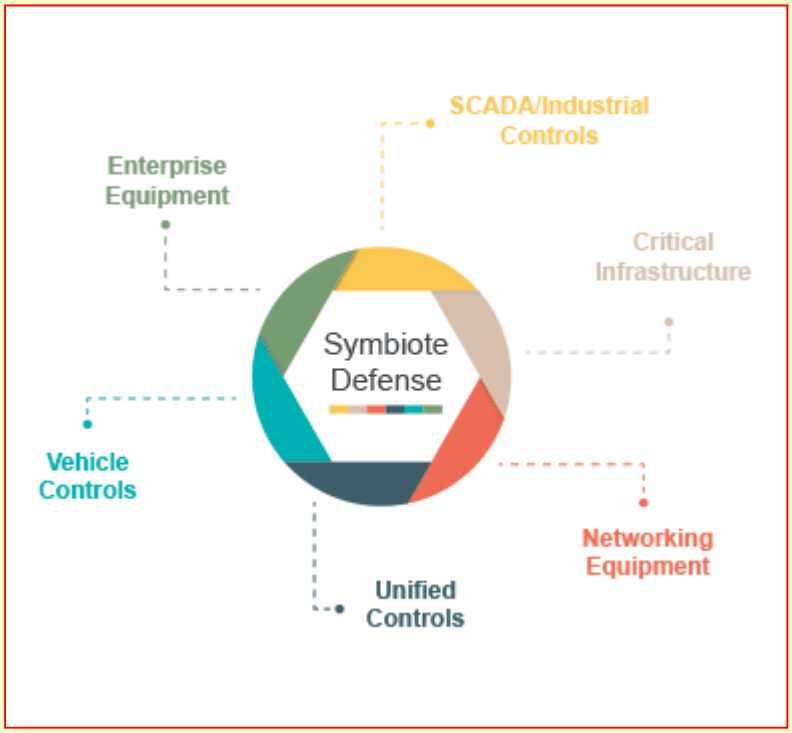
The cyber threat is more prominent than ever and a major consideration for most boardrooms across the globe. The fact is the skills gap is widening as there are just not enough people to do the job in hand. While there are, of course, downsides to "public sector poaching": these hires will typically have a 12-18 month notice period, on the whole, investing in ex-government and former military workers is a very smart - and cost-effective - way to bridge the widening cyber security skills gap. You just need to access them.

***Simon Kouttis** is head of cyber security practice an executive search firm Stott & May.*

DHS S&T Funded Technology Helps Protect Devices from Cyber Attacks

Source: http://www.dhs.gov/science-and-technology/dhs-st-funded-technology-helps-protect-devices-cyber-attacks

In 2011, a small group of university researchers working on securing embedded devices caught the attention of the Department of Homeland Security (DHS) Science and Technology Directorate (S&T).



That effort has since evolved into a one-of-a-kind technology – called Symbiote – that Hewlett-Packard (HP) recently licensed from Red Balloon Security, to protect its printers from cyber attacks.

The Symbiote technology will be integrated into HP's LaserJet Enterprise printers and multi-function printers. This new partnership between Red Balloon Security and HP is anticipated to secure technology in the mass market and increase security for a great number of devices

"What makes the Symbiote technology unique is the protection it offers for devices most organizations don't think to protect, like Voice over IP (VoIP) phones and printers," said S&T Cyber Security Division (CSD) Internet Measurement and Attack Modeling Program Manager Dr. Ann Cox.

The work was initially developed by researchers at Columbia University, who subsequently formed Red Balloon Security and continued developing the Symbiote technology. CSD's Broad Agency Announcement (BAA) 11-02 sought proposals in 14 technical topic areas aimed at improving security in both federal networks and the larger Internet, and developing new and enhanced technologies for detecting, preventing, and

responding to cyber-attacks on the nation's critical systems. S&T funded the Symbiote BAA proposal,

Symbiote is designed to detect intentional interference on many types of embedded system devices, such as routers, VoIP phones, point-of-sale devices, and so on. Red Balloon attracted the attention of HP after it decided to use a common HP printer for its research, completed a proof of concept, and published the results academically through Columbia University. HP has incorporated the Symbiote technology into their printer product line, providing protection to devices worldwide.

"The Symbiote technology is leading cybersecurity innovation," said Cox. "This technology is still developing new features to even the playing field between the attackers and defenders, allowing the defenders to pull ahead."

The technology features new capabilities that enable it to determine where the firmware has been penetrated and to lock down other devices on the same network to shield them from the attack. The technology was developed using some of the same techniques used by hackers, in effect, turning their own techniques against them. By leveraging these techniques, Symbiote is implemented with unique code every time it is placed in a new system. Each device has a different arrangement of Symbiote, making it hard for hackers to break into the device. The hacker must put the same level of effort into breaking into subsequent devices as they did to hack the first device.

The Symbiote technology is best used when incorporated into products during the manufacturing process. By design, this technology is appropriate for organizations that have a dedicated cybersecurity staff, but some sophisticated home users may be able to take advantage of the full benefit of the product.

The Symbiote technology will make a significant positive impact on the cyber landscape, said Cox.

▶ To learn more about CSD's research and development projects, visit www.dhs.gov/cyber-research.

Greece, Turkey Join NATO Cyber Defense Center

Source: http://i-hls.com/2015/11/finland-greece-turkey-now-part-of-nato-cyber-defense-center/

Nov 05 – **Finland, Greece and Turkey finalised their accession process to the NATO Cooperative Cyber Defense Center of Excellence (CCD COE). The Greek Republic and the Republic of Turkey joined as sponsoring nations and the Republic of Finland as a contributing participant.**

The ceremony marking the finalization of the three countries' accession to NATO's cyber defense agency was held on Tuesday and was attended by CCDCOE Director Sven Sakkov, Turkish Ambassador to Estonia Hayriye Kumaşçıoğlu, Permanent Secretary of the Finnish Ministry of Defense Gen. Arto Raty and Greek Ambassador to Estonia Constantine Catsambis.

Speaking at the ceremony, Sakkov highlighted that the cyber field has turned into a domain of warfare next to land, sea, air and space.

"The fact that the membership of the center is expanding, shows the growing importance of cyber defense. Cyber has evolved into a domain of warfare next to land, sea, air and space. It has changed our lives and will change warfare," he said. The NATO cyber defense center helps nations prepare for this future, Sakkov explained.

"Cyber poses a new global challenge that no nation can face alone. It is touching to see our flag fly side by side with so many others," said Gen. Arto Raty. Finland

contributes to the center because networking and cooperation are the only way to assure effective cyber defense, Räty added.

The Tallinn-based NATO Cooperative Cyber Defence Centre of Excellence is a NATO-accredited knowledge hub, think-tank and training facility. The international military organisation focuses on interdisciplinary applied research and development, as well as consultations, trainings and exercises in the field of cyber security. The center's mission is to enhance capability, cooperation and information-sharing between NATO, allies and partners in cyber defence.

Membership of the center is open to all allied nations. The Czech Republic, Estonia, France, Germany, Hungary, Italy, Latvia, Lithuania, Greece, the Netherlands, Poland, Slovakia, Spain, Turkey, the United Kingdom and the USA have signed on as sponsoring nations. Austria and Finland have joined the center as contributing participants. The center is funded and staffed jointly by these nations.

How Paris ISIS Terrorists May Have Used PlayStation 4 to Discuss and Plan Attacks

Source: http://www.forbes.com/sites/insertcoin/2015/11/14/why-the-paris-isis-terrorists-used-ps4-to-plan-attacks/

Following terrorist attacks in Paris which killed at least 127 people and left more than 300 injured, authorities are discovering just how the massacre was planned. And it may involve the most popular gaming console in the world, Sony's **PlayStation 4.**

The hunt for those responsible (eight terrorists were killed Saturday night, but accomplices may still be at large) led to a number of raids in nearby Brussels. Evidence reportedly turned up included at least one PlayStation 4 console.

Belgian federal home affairs minister Jan Jambon said outright that the PS4 is used by ISIS agents to communicate, and was selected due to the fact that it's notoriously hard to monitor. "PlayStation 4 is even more difficult to keep track of than WhatsApp," he said.

When the new generation of consoles launched, there were concerns that they would be *too* light on privacy, with peripherals like Microsoft MSFT +1.89%'s Kinect and PlayStation's Camera possibly having the ability to spy on users if say, the government wanted a window into your living room.

While the idea is certainly Orwellian, it's the non-peripheral based communication on consoles which may provide terrorists a channel to effectively converse with one another. The comparatively low-tech system may offer a more secure means of communication than even encrypted phone calls, texts and email.

While it remains unclear whether the Paris ISIS terrorists employed PS4 to communicate, there are a few options, from sending messages through the PlayStation Network (PSN) online gaming service and voice-chatting to even communicating through a specific game. Documents leaked by Edward Snowden in 2013 revealed that the NSA and CIA actually embedded themselves in games like *World of Warcraft* to infiltrate virtual terrorist meet-ups.

With PlayStation 4, it seems likely that simple voice communication could have worked just fine. It's still difficult for investigators to monitor IP-based voice systems compared to say, a simple cellphone. In 2010, the FBI pushed for access to all manner of Internet communications, including gaming chat systems. The FCC did not grant the FBI access to peer-to-peer communications, but the government agency did build its own rigs to record their communications in pursuit of criminals in organized chats, like a pedophile trying to lure kids via Xbox Live. Most consoles today come equipped with such capabilities, as nearly anything you do on your unit can be recorded if you want, in this age of YouTube and livestreaming.

The point is that terrorists could simply be in a PSN party together and chatting away mostly free from the fear that anyone is listening because of the difficulty and infrequency of governments eavesdropping on those forms of communication. It remains unclear just how much access the government has gotten to places like PSN and Xbox Live in the past few years, but whatever it is, it's likely still short of its ability to track more traditional forms of communication, such as cellphones and computers.

By last count, PSN alone had around 110 million users, 65 million of them active, making this no small pool of people. While government agencies can often build profiles of suspected terrorists based on their Internet or communication history, it's much harder to profile someone based on console usage, if that data is even accessible. Few users would visit extremist's sites in the PSN Web browser for instance or brag about future attacks in a public game lobby. There is no collection of games that really should raise "suspicion" about possible terrorist ties in an era where terrorism-filled *Call of Duty* titles are the best-selling games of the year, every year. How do you "profile" a gamer when information is not easy to access, and probably will tell you nothing even if you *could* get your hands on it?

The scary part of all this is that there are probably still a number of ways that terrorists could send messages to each other without speaking a word, if they really wanted to. **An ISIS agent could spell out an attack plan in *Super Mario Maker*'s coins and share it privately with a friend, or two *Call of Duty* players could write messages to each other on a wall in a disappearing spray of bullets.** It may sound ridiculous, but there are many in-game ways of non-verbal communication that would almost be impossible to track. To do so would require an FBI or NSA agent somehow tapping *all* the activity on an entire

console, not just voice and text chat, and that should not even be technically possible at this point.

While the makers of burner phones were once criticized for making it easier for criminals to communicate, it seems unlikely Microsoft and Sony will face the same scrutiny (not that they should). And yet, they may be inclined to start providing easier ways for governments to monitor specific accounts or consoles than what's readily available now. Because as it is, the most popular gaming devices also happen to be the most effective at connecting not just the world's friends, but the world's enemies as well.

ISIS Calls Anonymous Hackers Idiots Gives Lame Advice To AvoidGetting Hacked

Source: http://www.terrorismwatch.org/2015/11/isis-calls-anonymous-hackers-idiots.html

An ISIS-affiliated account on the messaging app Telegram has sent out a message about Anonymous' threat to launch its "biggest operation ever" against the terrorist group.

ISIS warns against the Anonymous threat

After the Paris terror attacks on Friday that left at least 129 people dead and hundreds more injured, the hacking collective Anonymous posted a video in which a person who claims to represent the group said, "Anonymous from all over the world will hunt you down." "We will launch the biggest operation ever against you," the masked person said. "Expect massive cyber attacks. War is declared. Get prepared."

A Telegram channel that's believed to be affiliated with ISIS hackers then sent out a message to its followers instructing them how to prevent getting hacked by Anonymous.

> ISIS idiots instructions to avoid #OpISIS #OpParis fighters. pic.twitter.com/EjNMAnSDNJ
> — GhostSecPl (@GhostSecPl) November 16, 2015
> "The #Anonymous hackers threatened in new video release that they will carry out a major hack operation on the Islamic State (idiots)," the statement read in part.

Instructions to avoid hacks

The message goes on to provide "instructions" on how to avoid potential hacks: Don't open any links unless sure of the source. Change Internet Protocol addresses "constantly." And "do not talk to people [you] don't know on Telegram" or through Twitter direct messaging. The message was then forwarded around to various other ISIS-affiliated Telegram channels. Anonymous started targeting extremists in January after the terror attacks on the satirical

French magazine Charlie Hebdo. The hackers worked to identify ISIS-linked social media accounts and take down extremist websites.

The Strongest Password: Atom-Based ID

Source: http://i-hls.com/2015/11/the-strongest-password-atom-based-id/

Nov 14 – **Scientists have discovered a way to authenticate or identify any object by generating an unbreakable ID based on atoms.** The technology, which is being patented at Lancaster University and commercialized through the spin-out company Quantum Base, uses next-generation nanomaterials to enable the unique identification of any product with guaranteed security.

The research, published in *Nature*'s *Scientific Reports*, uses atomic-scale imperfections which are impossible to clone as they comprise the unmanipulable building blocks of matter.

Current authentication solutions such as anti-counterfeit tags or password-protection base their security on replication difficulty, or on secrecy, and are renowned for being insecure and relatively easy to forge. For example, current anti-counterfeiting technology such as holograms can be imitated, and passwords can be stolen, hacked and intercepted.

The ground-breaking atomic-scale devices do not require passwords, and are impervious to cloning, making them the most secure system ever made. Coupled with the fact that they can be incorporated into any material makes them an ideal candidate to replace existing authentication technologies.

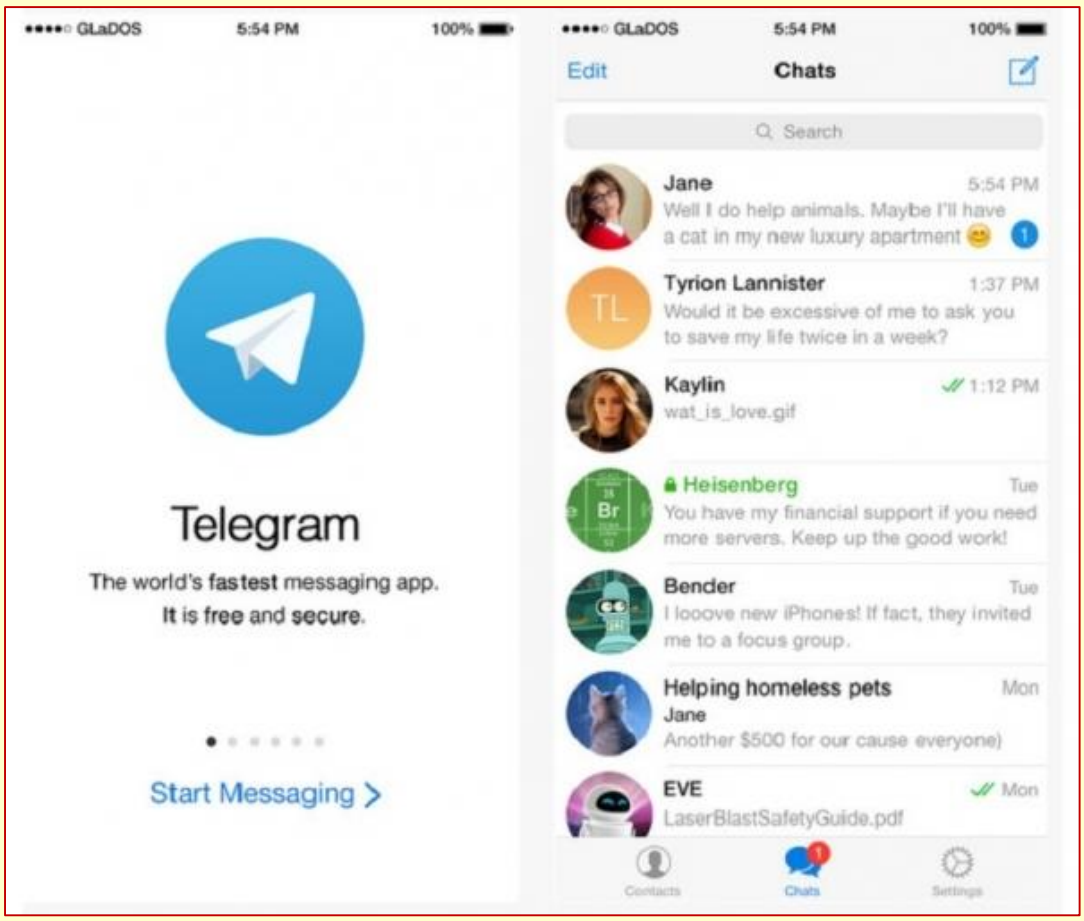
The reported Q-ID device, which uses an electronic measurement with CMOS compatible technology, can easily be integrated into existing chip manufacturing processes, enabling cost effective mass-production. The new devices also have many additional features such as the ability to track-and-trace a product throughout the supply chain, and individual addressability, allowing for marketing and quality control at the point of consumption.

Jonathan Roberts, a Lancaster University Physics Ph.D. student and first author in the publication said: "The invention involves the creation of devices with unique identities on a nano-scale employing state-of-art quantum technology. Each device we've made is unique, 100 percent secure and impossible to copy or clone."

Dr. Robert Young, the research leader at Lancaster University and co-founder of Quantum Base, said: "One could imagine our devices being used to identify a broad range of products, whether it is authentication of branded goods, SIM cards, important manufacturing components, the possibilities are endless."

Encrypted Messaging Apps on Spotlight as Possible Tools Used By Terrorists in Paris Attacks

Source: http://www.techtimes.com/articles/107586/20151117/encrypted-messaging-apps-on-spotlight-as-possible-tools-used-by-terrorists-in-paris-attacks.htm



Encrypted messaging apps such as Wickr, Signal and Telegram are back in the spotlight after the possibility that the Islamic State used the technology to coordinate the attacks in Paris. (Photo: Telegram | iTunes)

The deadly terrorist attacks in Paris have placed the spotlight back on encrypted messaging apps, and whether spies of the United States government should be given access to the encrypted messages that are being sent through the Internet.

Intelligence agencies have long been clamoring to be provided with so-called backdoors which would allow them to monitor e-mails, messages, calls, and other forms of electronic communications despite encryption. However, technology companies and privacy advocates have opposed the motion, with all legislative efforts to provide such backdoors so far being repelled.

A security official for the United States said that there has been no evidence yet that the attackers in Paris utilized a certain method of communication, and whether they utilized encryption for their communications.

However, several United States intelligence officials and lawmakers seized the opportunity to once again push for the implementation of backdoors.

"Silicon Valley has to look at its products because if you create a product that allows evil monsters to communicate in this way, to behead children, to strike innocents - whether it's at a game in a stadium, in a small restaurant in Paris, take down an airliner - that's a big problem," said United States Senator Dianne Feinstein.

Former Central Intelligence Agency deputy director said that the discussions regarding encryption have mostly been shaped by former National Security Agency contractor Edward Snowden and his allies, but a new chapter will unfold after the events in Paris.

Obama administration officials are claiming, despite there being no definite evidence yet, that the Islamic State used several encryption technologies over the previous one and a half years. Many of these technologies could not be cracked by the National Security Agency.

Some of the most powerful encryption technologies are publicly available for free, including apps such as Wickr, Signal and Telegram. Militants from the Islamic State utilized Telegram a couple of weeks ago to claim the responsibility for the Russian jet crash in the Sinai Peninsula, and then used the app again to claim the responsibility for the attacks in Paris. It is not clear, however, if the group also uses the secret messaging service of Telegram to hide private messages between its members.

John Brennan, the director of the CIA, said that the attacks in Paris were a wake-up call on the issue of encrypted messaging apps, adding that the focus on privacy was limiting the ability of intelligence agencies to prevent such acts of terrorism.

Cybersecurity experts believe that similar comments would be made by officials in the future, especially if it is confirmed that the attackers utilized encrypted messaging apps for communications.

"If you want controls on encryption, and you see an attack where encryption might have been used, then you are going to say something," said Worcester Polytechnic Institute in Massachusetts professor of cybersecurity policy Susan Landau.

FEMA assessing over-the-air broadcast alerting technology

Source: http://www.homelandsecuritynewswire.com/dr20151021-fema-assessing-overtheair-broadcast-alerting-technology

The Department of Homeland Security (DHS) Federal Emergency Management Agency (FEMA) National Continuity Programs' Integrated Public Alert and Warning System Division (IPAWS) has begun to assess the feasibility of a public alert and warning capability which is being developed in the private sector.

FEMA says that new technologies could deliver detailed emergency information to the public with pictures and videos of evacuation routes, storm tracks, and shelter information — increasing community preparedness before, during, and after a disaster. The media alerts will be able to include multilingual and multi-format information to warn non-English speaking populations and people with access and functional needs.

"FEMA is committed to working with the private sector to examine and improve future alerts and warnings," said Roger Stone, Acting Assistant Administrator for National Continuity Programs. "New systems could someday include pictures and video as part of the advanced alert and warning information provided to the general public."

One such technology being considered is the Advanced Warning and Response Network (AWARN). AWARN works by using advanced capabilities in the next generation of digital television broadcast system called ATSC 3.0 being standardized by the Advanced Television Systems Committee. The **emerging television broadcast standard** provides for the transmission of large media rich, data messages over-the-air to mobile, portable, and fixed television and video devices without interrupting ongoing television shows.

FEMA notes that its IPAWS is a national system for local alerting. IPAWS enables authorities at all levels of government to alert and warn people in areas endangered by disasters. IPAWS is used by federal, state, and local authorities to send emergency alerts to cellular phones as Wireless Emergency Alerts (WEAs), to radio and television as Emergency Alert System (EAS) broadcasts, to NOAA Weather Radios, and to an All-Hazards Alert and Information Feed for Internet applications, services, and Web sites.

Location Data for First Responders

Source: http://i-hls.com/2015/10/location-data-for-first-responders/

Oct 22 – **How can first responders be sure they've taken care of everyone in the scene? And what if one of the injured, unconscious behind the door at the end of the hall, has escaped them?**

Offsite Vision Holdings (OSVH), who specializes in real-time security and safety solutions, has come up with a way to allow first responders to scan the place completely without running all across the building, thus saving time, effort and human lives.

The company has announced the launch of **EmergenZ Evacuation**, a new product that allows emergency responders and security personnel the ability to account for people during evacuation events by knowing who is left in the building and their location. This new product offers first responders access to location data in real-time 24/7 as well as a real-time repost about entrances and exists in the building. This way, search and rescue teams can quickly detect anyone in a certain facility and treat them accordingly.

This cost-effective solution is part of the EmergenZ real-time security and safety solutions product suite which provides the vital information that first stand emergency response teams and security personnel need to gain immediate and accurate data to identify, respond and mitigate the situation quickly and effectively. First responders are basically getting another important piece of the puzzle that improves their understanding of any emergency situation, as it helps them see what's beyond sight.

"We are very excited to be launching EmergenZ Evacuation to help facilities throughout the world prepare for an emergency situation. Unfortunately, with the increase in workplace violence and active shooter incidents over the last few years, facilities need to be prepared now more than ever in the event of an emergency situation. The key to saving lives is being prepared," states William Lenahan, OSVH's CEO.

Remember DoD's Counter-Zombie Plan? It's Actually a 'Brilliant' Preparedness, Mitigation, and Response Strategy for New and Unforeseen Threats

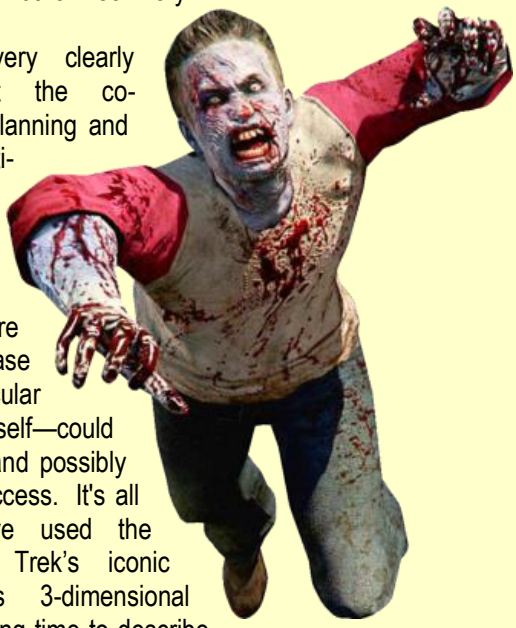
By Dr. Pietro D. Marghella

Source: http://www.hstoday.us/focused-topics/emergency-managementdisaster-preparedness/single-article-page/remember-dods-counter-zombie-plan-it-s-actually-a-brilliant-preparedness-mitigation-and-response-strategy-for-new-and-unforeseen-threats/e4aabafcf2efc931df7ebb2d78.html

It's been many months since the Defense Department's fictitious *CONPLAN 8888-11, Counter-Zombie Defense*, was made public and held up to ridicule –- some declaring it another example of wasteful Pentagon spending. I mean, come on, frittering money on a fictitious plan for countering a zombie apocalypse? But the fact is, *CONPLAN 8888-11* is brilliant on so many levels. My first reaction was I'm so incredibly proud of our military. This effort is like a "knowledge force multiplier" on the issues of planning, crisis response and asymmetrical threat.

Probably the best and most important thing they did with *CONPLAN 8888-11* was to make it available on Intellipedia so both the American public, and, more importantly, the emergency management community could look at and work with the best example of a CONPLAN template they could possibly find.

As the authors' of the fictitious counter-zombie plan noted -- it's funny and entertaining. It was designed that way so its concepts would be entertaining to digest. Even though a 6th grader could probably grasp the underlying metaphor for "terrorist" and a novel "pathogenic threat," by using humor and a metaphoric zombie threat characterization embedded in pop culture, they removed real fear from the equation and (probably without the less sophisticated reader understanding it) walked those who "consume" it through the logical process of threat characterization and the requirements associated with preparedness, mitigation response and recovery against new, unforeseen … and otherwise very fearful threats.



The plan also very clearly demonstrated that the co-mingled efforts of planning and response are multi- or, even hyper-dimensional efforts, where no single silo of a critical infrastructure sector—or, in the case of this particular scenario, society itself—could work in a vacuum and possibly hope to achieve success. It's all co-mingled. I have used the analogy of Star Trek's iconic character, Spock's 3-dimensional chess game for a long time to describe the complexities of planning and response, i.e., when one piece is moved on one layer or dimension of the game, it has a cause-and-effect impact on another that must be accommodated.

The military has understood this almost intuitively for as long as they have done operational planning, but it is a concept that has eluded us in the domestic Environment. By using a walking dead scenario, they have "universalized" the asymmetrical threat that is now endemic to our environment in the

post-911 era. While the scenario is ludicrous, the reader nevertheless is left with a better grasp of the notion of a threat that could affect us all -- and that only by beginning to plan (at the personal level, at the home level, at the community level, etc.) can we hope to achieve resilience against any kind of new, fantastical scenarios.

When the media first reported DoD's counter-zombie plan last year, they didn't seem to get it. The media, pundits and talking heads mocked the CONPLAN as a waste of time and money. But the fact is, this was probably the brainchild of some *über*-smart major who should be allowed to pass 'Go' and be directly promoted to at least 2-star rank!

With its fictitious zombie CONPLAN, DoD went "Aikido" on us—but most of the public, and certainly the media -- didn't grasp the implications of what was conceptualized in the plan. Aikido is counter-intuitive to the normal practitioner of the (percussion) martial arts. Instead of using force against a threat, the "Aikidoka" uses the force generated by the attacker to throw the attacker off balance with little or no effort. As the practitioner moves within what is referred to as the "dynamic sphere," he simply directs the energy of the attack in exactly the direction it was already going. But since the attacker doesn't expect this—he expects force will be met with reciprocal force—he effectively gives his balance away, and in doing so, loses the engagement.

So, how does this compare with what the authors of this counter-zombie plan did with the plan? The universal adversary—and novel diseases—have entered our dynamic sphere (i.e., the United States, our Western Allies, the planet even) in the 4th generation of warfare. There is no getting around that anymore. We could approach emerging threat(s) in our classically trained manner (the manner that may have worked in the 3rd generation of warfare dominated by force-on-force engagement with non-asymmetrical weapons systems), and try and use antiquated tactics, techniques, policies and procedures (TTP&P). But this plan proves (to me, at least) that there is emerging recognition that those TTP&Ps that worked for a long dead enemy will simply cause us to have our balance taken from us in short order in the modern era—something we clearly cannot afford to let happen.

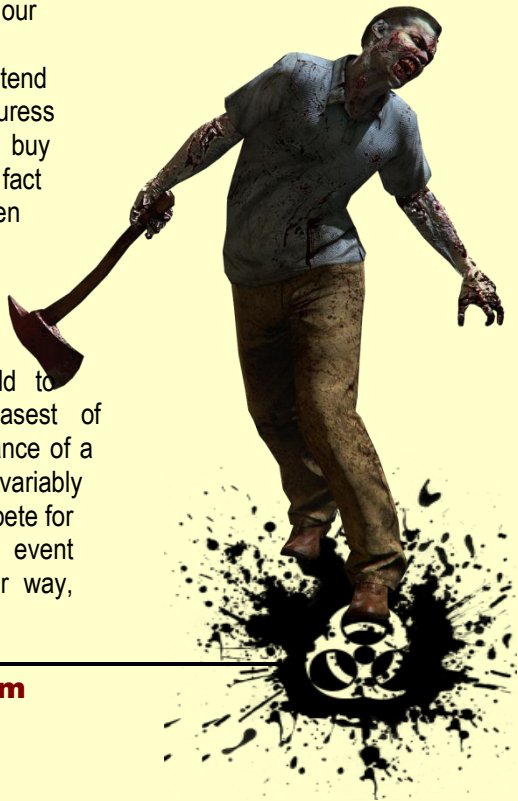
So, what do you do? Well, you break the mold. You engage the threat through clever metaphor; pull, then push it in the direction you can control; take the thinking about the threat out of the black world of clandestine operations and into the mainstream of society; and engage the common citizen in the process of improving his or her own posture of preparedness right down to the most base and micropolitan level of our society. I'll repeat—*it's brilliant*!

Somebody very smart was behind this. This should actually be held up as a groundbreaking, forward moving effort in the realignment of our approach to tional security in the 21st Century.

A friend of mine named Peter Hitt once described the definition of the word "resilience" as, 'The ability to live as normally as possible in an abnormal environment.' When you watch virtually any zombie movie or TV series like, "The Walking Dead," what are the humans doing at all times (other than decapitating, blowing up or blowing away the zombies)? They're trying to do just what Peter described—live as normally as possible while the rest of the world has gone the way of the living dead. They still need to eat and drink, find shelter and medical care, and protect their wives and children. All kidding aside, these are the base pursuits of our existence that American psychologist Abraham Maslow described in his "*Hierarchy of Needs*" in 1947.

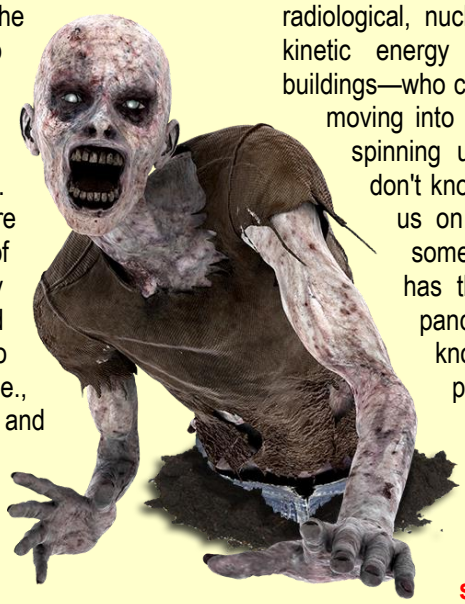
I flexed the "*Hierarchy of Needs*" in previous writings to show that when the environmental duress of a disaster presses down on our society, we tend to reflexively revert to those base elements of our existence.

However, since we tend not to think about duress on a daily basis, or buy into the very real fact that risk -- even fantastical risk -- has increased in our environment, we don't take the measures we should to prepare for the basest of requirements in advance of a disaster. We invariably struggle, and/or compete for them, *when* the event occurs. Said another way,



by failing to engage in any sort of pre-event planning, our chances of mounting an adequate response diminish in equal -- but inverse -- proportion to the impact and magnitude of the event.

With the subtle craft of a master, whoever is responsible for writing the Zombie Plan is suggesting to its consumers that we have, indeed, entered into a paradigm shift in terms of dealing with emerging threats. That is, the only way we are going to change our posture of preparedness is by understanding that each and every one of us has to embrace the zombie (i.e., believe that a threat is real), and then figure out what we have to do keep the monsters at bay and still live as normally as possible in a new-normal, *albeit very abnormal*, world.



At the height of the Cold War, it could be argued that the nuclear Sword of Damocles hung precariously an inch from each of our collective necks as citizens of this planet. Yet, the threat was a known and familiar one. We practiced to make our responses reflexive; we had alarming mechanisms to alert us to increased threat; and we talked about it *all the time*.

We have none of that now. A comparable threat, today, is one, big, very frightening unknown to us. We don't know what we might be attacked with next (chemical, biological, radiological, nuclear, or more high-explosive, kinetic energy weapons ripping into tall buildings—who can tell?). We can't see armies moving into position any more, or ICBMs spinning up in their launch silos. We don't know if the guy sneezing next to us on a plane might be shedding some new and virulent virus that has the ability to create the next pandemic. And we really don't know if the chicken zombie (CZ) phenomenon will one day manifest itself in the human species. Can anyone say definitively it won't?

What we should know—and what this plan suggests—is that one way or another, we have to embrace readiness at a very personal level if we're going to have any hope of getting through whatever the next big event is going to be. And, that we shouldn't be waiting for some wacky, cosmic-ultra-top-secret plan that the US government may—or, hmm, may not, have—to come riding in to the rescue when the monsters appear on the horizon.

Dr. Pietro (Peter) D. Marghella *currently serves as the Senior Advisor for Medical Planning and Preparedness for the International Medical Corps, the largest direct response medical and public health non-governmental organization in the United States. He previously served as director of the New York State Office of Emergency Management.*

A career naval officer, Marghella served as a plans, operations and medical intelligence officer in the Navy's Medical Service Corps, retiring as the Director of Medical Contingency Operations for the Office of the Secretary of Defense. Previous assignments included Chief of Medical Plans and Operations for the Joint Chiefs of Staff; Chief of Medical Plans and Intelligence for the US Pacific Command; and Chief of Medical Plans and Intelligence for the Office of the Chief of Naval Operations. His national-level planning credentials include authorship of the nation's first Catastrophic Incident Response Plan (response to acts of domestic nuclear terrorism) and the National Smallpox Response Plan.

Dubai firefighters to tackle high-rise fires with Jetpacks

Source: http://www.gizmag.com/martin-jetpack-dubai-firefighters/40368

Nov 12 – Fires in high-rise buildings can be very problematic. It can be difficult to move around the building, to quickly get equipment to where it needs to be and even to communicate with people inside. Dubai, a place with lots of towering constructions, plans to tackle this by giving Jetpacks to its firefighters.

The country's Directorate of Civil Defence has signed a memorandum of understanding with Martin Aircraft Company for the planned initial delivery of up to 20 Jetpacks and two training simulators. The proposed deal will also include initial training services and operational support.

Martin Jetpacks have been developed with first responder use in mind. They can be flown by a pilot or via remote control, take off and land vertically, operate in confined spaces (such as close to or between buildings or near trees) and carry commercial payloads of up to 120 kg (265 lb).

This functionality means the Jetpacks can provide a variety of first response services. For example, they can be used for surveillance or observation (such as to determine the focus of a fire), transporting equipment to where it is required, rescuing individuals or deploying specialist teams.

The agreement was signed earlier this week at the Dubai Air Show.

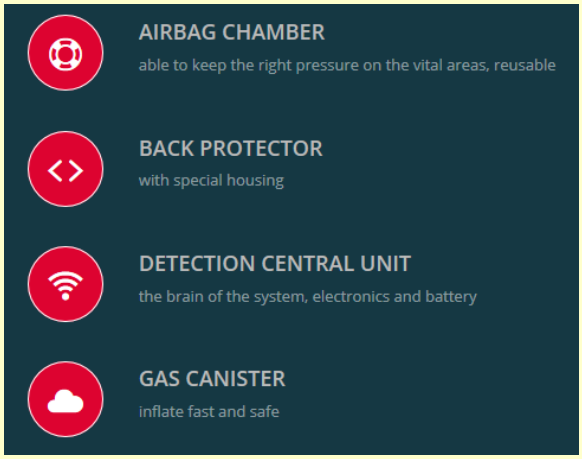
Wireless technology enables advanced up protective clothing

Source: http://www.homelandsecuritynewswire.com/dr20151113-wireless-technology-enables-advanced-up-protective-clothing

Nov 13 – Combining the latest advances in sensor and wireless technology with comfortable protective clothing has opened up new partnership possibilities across a range of sectors. Numerous end users stand to benefit from the inclusion of smart technology in protective clothing.

For example, while French high-tech start-up IN&MOTION has pioneered intelligent active protection systems for ski racers, the company's ambitions do not stop at the chair lift. "We wanted to investigate whether this technology platform could be used by end users in different markets," explains project coordinator Rémi Thomas, co-founder of IN&MOTION.

The wearable ski racing air bags developed by the company combine sensor and wireless communication technology that can detect unavoidable falls and inflate in less than 100 milliseconds. User can reactivate the device after deployment, thanks to easy-to-handle consumable parts, making it cost-effective.



The innovation will be used at international racing events as of the 2015-16 ski season. With the right partners, Thomas is confident that the sensor and wireless technology platform can be adjusted to suit motorcyclists.

CORDIS says that to this end, the recently completed six-month EU-funded INE IAPS project enabled the company to carry out an assessment of the technical challenges and market potential of adapting the airbags to suit the needs of motorcyclists. The risk of fatality or sustaining serious injury in motorcycling accidents remains poorly addressed by existing body protection devices, which have to date failed to adequately integrate sensor and wireless technologies.

"We spent time discussing these issues with stakeholders, including end users (motorbike riders) and equipment and clothing manufacturers," explains Thomas. "The feedback has been encouraging in that, while there is a clear demand for high tech protection, there is still dissatisfaction with what is currently available on the market."

This was the first stage of the project; establishing that a viable market exists for advanced protective clothing in the motorcycling sector. The second stage involved analyzing technical challenges and seeing what elements of the company's platform might need to adapted in order to better suit the needs of bikers.

Feedback from the industry here has proved very useful. "We are a business to business company," explains Thomas. "To us, it makes sense to combine our technological expertise with the knowledge of companies that understand the market better and know exactly what end users are looking for." The next step will be to develop and tweak the technology to suit the specific needs of this sector, and to find partners capable of turning the concept of smart protective motorcycle clothing into a commercial reality.

Thomas said he is also keen to organize simulated tests in order to provide scientific proof of the airbag's benefits for motorcyclists. This has not been done to date, and would strengthen the commercial positioning of the product when it comes to market. "We have identified a number of potential institutions,' he says. 'All this, of course, takes time and investment."

6 Information Management Challenges in an Emergency Response

Source: http://www.d4h.org/blog/post/20150216-6-information-management-challenges-in-an-emergency-response

When an incident occurs, both incident responders and managers are faced with high volumes of information. Their priority is to bring the incident to a swift ending. This means that efficient management of information can relieve some pressure. There are however a

number of common information managment challenges associated with incident response. They include;

1. Paper Based information Gathering

When an incident occurs, a high volume of information is traditionally captured by completing paper-based forms by hand, which are later processed. The biggest shortcomings of the paper-based system is the poor quality of the records, a lack of contextual information and difficulty in instantly analysing any data captured.

2. Time Stamping Information

After an incident has occurred there is a need to report on the events. A major difficulty is recording the times and sequence in which events and tasks occurred. When using paper a possibility is the use of rubber stamps, these are often used in offices to stamp the current date, however this is a cumbersome task. The most efficient method is using a digital timestamp, the time at which an event is recorded by a computer.

3. Recording of Tasks

Task management is the process of managing a task through its life cycle. Effective task management requires managing all aspects of a task, including its status, priority, time, human and financial resources, notifications and so on. These can be lumped together broadly into the basic activities of task management. The difficulty during a high stakes event is that tasks are assigned to multiple individuals or teams and there are a number of stages to monitor from who has been assigned the task to wether its completed/failed.

4. Access to Documentation

Often response plans are bulky paper documents in folders that are stored on a bookcase in an operation centre. When needed such folders may not be available immediately at the scene and depending on the scenario personnel may not be familiar with the relevant parts of a plan they are to enact.

5. Managing Multiple Sources of Information

During an incident, information is everywhere and arriving in many forms. Managers may be receiving radio communications, video streams, photos, calls, emails, texts, alarm

notifications, and paper forms. Finding the best method to manage it is a major challenge. The ideal solution when managing such large volumes of information is to capture all the data in an information management system which acts as a single source of truth.

6. Quickly Querying Information

Being able to effectively query information captured during an incident can be difficult as it is coming from multiple sources. However, when managed effectively it can improve an organizations situational awareness. Situational awareness is more complex than simply noticing what is happening around you. An emergency manager must capture clues and cues in the emergency environment, make sense of the information, and predict what will happen next.

Demonstrating technologies for disaster response

Source: http://www.homelandsecuritynewswire.com/dr20151119-demonstrating-technologies-for-disaster-response

Nov 19 – Radiological incidents such as Chernobyl and Fukushima illustrate the need for effective coordination of federal, state, and local agencies in response efforts. S&T says that as part of the U.S. efforts, earlier this year, the Department of Homeland Security (DHS) Science and Technology Directorate's (S&T) National Urban Security Technology Laboratory (NUSTL) and the Environmental Protection Agency (EPA) demonstrated new technology developments at the Columbus, Ohio, Battelle Memorial Institute facility that will enable more effective radiological decontamination.

This demonstration was made possible through a partnership between NUSTL and EPA to research methods, best practices, and technologies for containing contamination and mitigating the hazard of radiation.

"It is vital for first responder agencies to understand the cleanup options available for events of all sizes," explained NUSTL Radiological/Nuclear Response and Recovery (RNRR) Division Director Ben Stevenson. "When supporting local agencies and first responders for radiological response and recovery, it is important that S&T provide them with good scientific guidance and technology, but equally important that we connect them to experts and specialized federal assets that can support their operations and decision-making during an emergency."

S&T notes that the Radiological Gross Decontamination and Waste Management First Responder Application project with the EPA is part of a NUSTL-managed research and development portfolio for S&T's First Responders Group. It is focused on increasing local capabilities to respond to and recover from radiological incidents.

"Our partnership with DHS provided us with great opportunities to interface directly with local responders, providing them with tools for a more effective response that are not an additional burden to them—especially since they will be the first boots on the ground after an incident and will be primarily focused on saving lives and property," said EPA environmental scientist Sang Don Lee. "These tools will also integrate into their activities as seamlessly as possible and into the activities of other responders who arrive later. This may dramatically speed up and lower the cost of the response and recovery, and help assure the public that their community will be able to bounce back after one of these incidents."

The demonstration, which included state, local, and federal responders; expert scientists from national laboratories; and industry representatives, demonstrated how to apply these technologies on a city-wide scale using equipment already on hand, while minimizing the effects of radiological contaminants.

"While any radiological incident will have specific response and recovery operations, understanding the available technology in the toolbox is important in advance of an incident to ensure an effective and efficient response and recovery," said Stevenson.

Responders gave positive feedback to EPA and DHS S&T about the structure of the event and information provided, and that will likely lead to future similar events to highlight available technology through field demonstrations. Additionally, lessons learned are being compiled and will be available in

the near future in a report that will be posted to the firstresponder.gov Web site.

"We've strived for a long time to extend our cleanup work to all phases of radiological response and all levels of responders — federal, State, local, and tribal," said Matthew Magnuson, EPA research chemist. "Collaborating with DHS allowed us a unique opportunity to turn this goal into reality and our research in this area into practice."

As it was in the days of Noah ...

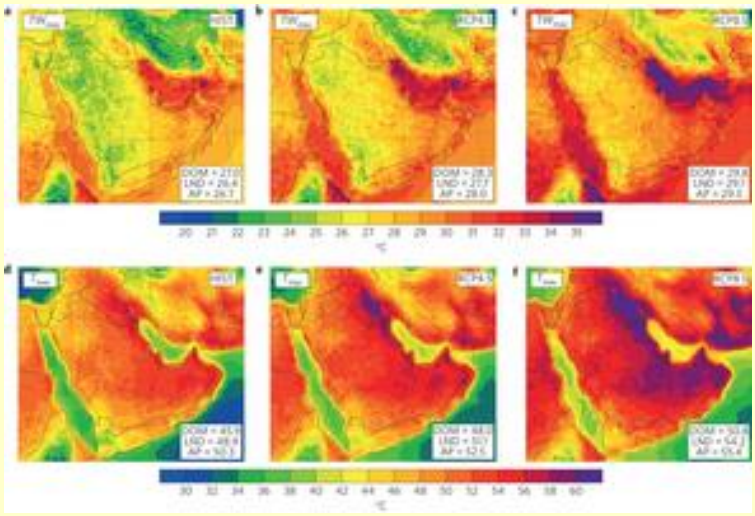
Persian Gulf could experience deadly heat

By David L. Chandler

Source: http://www.homelandsecuritynewswire.com/dr20151028-study-persian-gulf-could-experience-deadly-heat

Oct 28 – Within this century, parts of the Persian Gulf region could be hit with unprecedented events of deadly heat as a result of climate change, according to a study of high-resolution climate models. The research reveals details of a business-as-usual scenario for greenhouse gas emissions, but also shows that curbing emissions could forestall these deadly temperature extremes.

The study, published in the journal *Nature Climate Change*, was carried out by Elfatih Eltahir, a professor of civil and environmental engineering at MIT, and Jeremy Pal, PhD '01, at Loyola Marymount University. They conclude that conditions in the Persian Gulf region, including its shallow water and intense sun, make it "a specific regional hotspot where climate change, in absence of significant mitigation, is likely to severely impact human habitability in the future."



Running high-resolution versions of standard climate models, Eltahir and Pal found that many major cities in the region could exceed a tipping point for human survival, even in shaded and well-ventilated spaces. Eltahir says this threshold "has, as far as we know … never been reported for any location on Earth."

That tipping point involves a measurement called the "wet-bulb

temperature" that combines temperature and humidity, reflecting conditions the human body could maintain without artificial cooling. That threshold for survival for more than six unprotected hours is 35 degrees Celsius, or about 95 degrees Fahrenheit, according to recently published research. (The equivalent number in the National Weather Service's more commonly used "heat index" would be about 165 F.)

This limit was almost reached this summer, at the end of an extreme, weeklong heat wave in the region: On 31 July, the wet-bulb temperature in Bandahr Mashrahr, Iran, hit 34.6 C — just a fraction below the threshold, for an hour or less.

But the severe danger to human health and life occurs when such temperatures are sustained for several hours, Eltahir says — which the models show would occur several times in a 30-year period toward the end of the century under the business-as-usual scenario used as a benchmark by the Intergovernmental Panel on Climate Change.

The Persian Gulf region is especially vulnerable, the researchers say, because of a combination of low elevations, clear sky, water body that increases heat absorption, and the shallowness of the Persian Gulf itself, which produces high water temperatures that lead to strong evaporation and very high humidity.

The models show that by the latter part of this century, major cities such as Doha, Qatar, Abu Dhabi, and Dubai in the United Arab Emirates, and Bandar Abbas, Iran, could exceed the 35 C threshold several times over a 30-year period. What's more, Eltahir says, hot summer conditions that now occur once every twenty days or so "will characterize the usual summer day in the future."

While the other side of the Arabian Peninsula, adjacent to the Red Sea, would see less extreme heat, the projections show that dangerous extremes are also likely there, reaching wet-bulb temperatures of 32 to 34 C. This could be a particular concern, the authors note, because the annual Hajj, or annual Islamic pilgrimage to Mecca — when as many as 2 million pilgrims take part in rituals that include standing outdoors for a full day of prayer — sometimes occurs during these hot months.

While many in the Persian Gulf's wealthier states might be able to adapt to new climate extremes, poorer areas, such as Yemen, might be less able to cope with such extremes, the authors say.

Christoph Schaer, a professor of atmospheric and climate science at ETH Zurich who was not involved in this study, provided an independent commentary in the journal, writing that while deadly heat waves have occurred recently in Chicago, Russia, and Europe, in these cases infants and the elderly were most affected. The new study, Schaer writes, "concerns another category of heat waves — one that may be fatal to everybody affected, even to young and fit individuals under shaded and well-ventilated outdoor conditions."

Schaer writes that "the new study shows that the threats to human health may be much more severe than previously thought, and may materialize already in the current century." He told MIT News, "I think the study is of great importance, since it indicates where heat waves could get worst if climate change proceeds."

The research was supported by the Kuwait Foundation for the Advancement of Science.

— Read more in Jeremy S. Pal and Elfatih A. B. Eltahir, "Future temperature in southwest Asia projected to exceed a threshold for human adaptability," Nature Climate Change (26 October 2015)

Climate change heightening the risk of conflict and war

Source: http://www.homelandsecuritynewswire.com/dr20151103-climate-change-heightening-the-risk-of-conflict-and-war

Nov 03 – **Thirty of Australia's leading minds from defense, academia, policy think tanks, and other government agencies have joined together for discussions over two days last week for Australia's first climate security summit.**

The roundtable members wrestled with many issues of fundamental

importance to Australia's national security, including the risks posed by climate change to geopolitical stability, the challenges faced by the Australian Defense Force (ADF) in providing humanitarian assistance in response to more frequent and extreme severe weather events, and how the ADF can best prepare for the considerable strategic risk and uncertainty posed by climate change.

Australia's Climate Council notes that increasing temperatures, rising sea levels, changing rainfall patterns, and more frequent and severe extreme weather events are heightening the risk of conflict and increasing the displacement of people.

One of the primary areas of discussion was the steps that need to be taken to align Australia's defense preparedness with allies such as the United States and the United Kingdom.

Summit co-chairs, former ADF chief Admiral Chris Barrie (Ret.) and the Climate Council's Professor Will Steffen, joined by key summit participants Rear Admiral David Titley (Ret.) and Rear Admiral Neil Morisetti (Ret.), issued the following co-chair statement:

1. The Australian government should take immediate and significant steps to mainstream climate change into defense planning

- Governments in the United Kingdom and the United States have taken significant legislative and strategic steps to ensure that climate change is integrated into defense planning. The United States has mandated that their military forces address the risks of climate change as a routine part of all mission planning.
- In Australia, comparatively less action is being taken by the government to ensure that the ADF is prepared for the security risks posed by climate change.
- The upcoming Australian Defense White Paper must address the security implications posed by a changing climate.
- Security is a whole of government task and therefore the challenge needs to be viewed more broadly than the ADF.

2. Climate change is exacerbating tensions in areas with existing global instability, increasing the risk of conflict, and changing the nature of ADF missions

- The impacts of climate change can exacerbate other stresses, like poverty, economic shocks, and unstable institutions, to make crises worse, particularly in countries with poor governance or existing instability.
- For instance, increasing extreme weather events can reduce the availability of food. Extreme weather and water scarcity contributed to soaring food prices, which saw food riots erupt across Africa and the Middle East in 2008. Rising food prices in 2011 have also been identified as one of the factors that destabilized the Middle East, leading, for example, to the Arab Spring.

3. The Australian Defense Force is already under pressure from climate change

- Australia and the Asia-Pacific region are particularly vulnerable to climate change. The ADF is increasingly called upon to deliver humanitarian assistance in response to the rise in the frequency and severity of extreme weather events and their impacts both at home and in the region. In serious cases the ADF coordinates with civilian disaster relief organizations in Australia and with a range of military and civilian organization in other countries to provide assistance.
- Extreme weather could also affect the ADF's readiness and capability by disabling critical military and civilian infrastructure at times when rapid mobilization is needed. Defense property (military bases) are also at risk from sea- level rise and extreme weather.
- Rising temperatures and more frequent and intense heatwaves have implications for the health of Australia's military personnel when undertaking training and conducting military exercises.

4. Limiting the security consequences of a changing climate requires strong action by countries like Australia

- Global emissions must start tracking strongly downward this decade if there is to be a chance of keeping the warming of the planet to below 2°C, and thereby limit the severity of climate change and its implications for security.
- The upcoming COP21 conference in Paris is a crucial turning point that must build momentum towards rapid and deep decarbonization of the global economy over the coming decades.
- We must adapt to the inevitable changes that are

already occurring while working hard to minimize the long-term changes, some of which could be massive, abrupt and disruptive.

The organizers of the climate security summit said that the bottom line is clear and compelling:Climate change is far more than "just" an environmental issue; it fundamentally changes our relationship with food and water, which is essential for our well-being and for the viability of nearly all other forms of life. "We have collectively built and optimized all of human civilization for the relatively stable climate that has existed for thousands of years, starting at the end of the last ice age," the organizers of the summit said. "That climate is now changing rapidly."

The summit organizers quote Brigadier-General Wendell Christopher King (Ret.), the Chief Academic Officer at the U.S. Army's Command and General Staff College, who said: "[Climate change] is like getting embroiled in a war that lasts 100 years….There is no exit-strategy."

— Read more in The Australian Climate Security Summit: Exploring the significant and growing security challenges presented by a changing climate (Climate Council, 2015)