International CBRNE Institute

CBRNE NEWSLETTER TERRORISM

E-Journal for CBRNE & CT First Responders

August 2016

www.cbrne-terrorism-newsletter.com

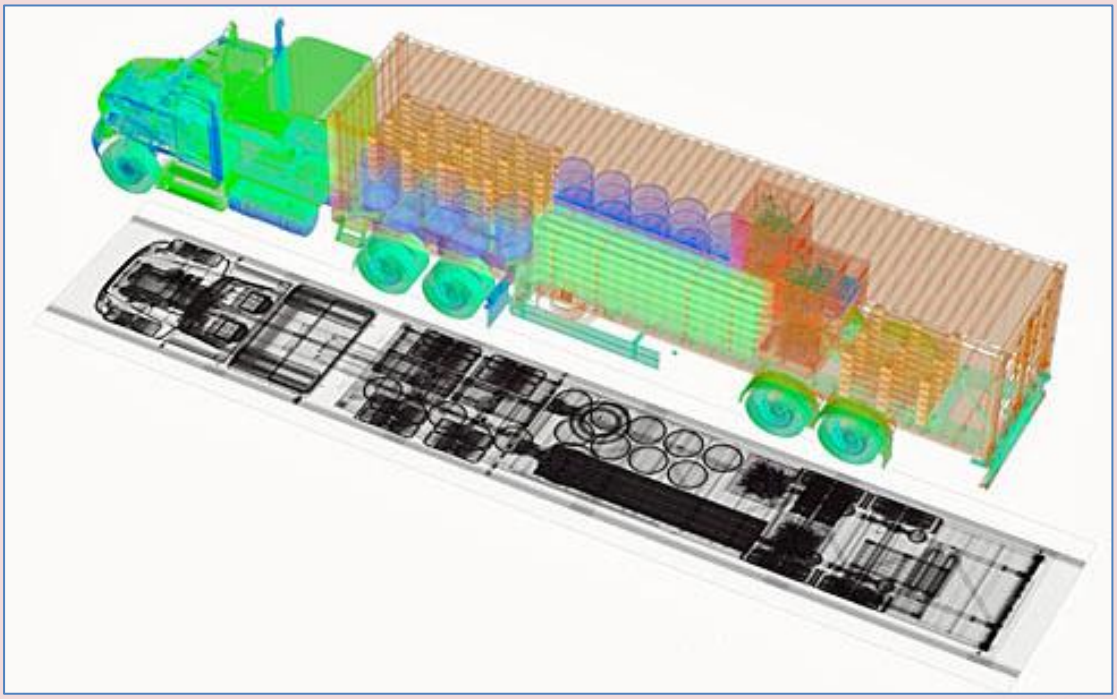
New Cargo Radiation Detection Technology

Source: http://i-hls.com/2016/07/new-cargo-radiation-detection-technology/

July 23 – Seaports customs and security professionals might sometimes miss contraband attempts, including radiological materials. The problem was hightened during a US congressional hearing, when officials emphasized the gaps in securing nuclear and radiological materials around the globe, and acknowledged the challenges that the U.S. faces in protecting its ports from smuggled materials.

Passport Systems, Inc. developed the fixed cargo scanner SmartScan 3D, a radiation detection technology that can help domestic and foreign seaports thwart nuclear terrorists seeking to transport radioactive materials.

Robert Ledoux, President, CEO, and Director of Passport Systems, Inc., said that "at the hearing, subcommittee members cited the need for technology that can accurately detect nuclear threats and



contraband without significantly slowing the shipping process." He added that the technology was already being deployed at the port in Boston, and is ready to be deployed to other ports in the U.S. and internationally.

According to PR Newswire, he cargo scanner can protect people and property from dirty bombs and other nuclear threats. The system automatically identifies any radioactive material, including "actinides" that may signal a weapon of mass destruction or smuggled special nuclear materials, after the cargo has been unloaded onto conveyances.

The non-intrusive cargo inspections also detect explosives and contraband such as drugs, tobacco, and firearms.

Passport will this fall unveil SmartScan at the Massachusetts Port Authority, Port of Boston's Conley Container Terminal. The facility is part of a U.S. Department of Homeland Security, Domestic Nuclear Detection Office (DNDO) project

As noted at the subcommittee hearing, a limited X-ray scanning process is used at most ports today. Dense or thick objects, which could hide nuclear threats or contraband, require that individuals open the containers and inspect the objects by hand; it slows the shipping process by hours and the process could be dangerous for inspectors.

By contrast, **SmartScan doesn't require that containers be opened.** The technology scans a container, provides a three-dimensional map of the cargo, and sends alerts to flag suspicious cargo. Within minutes, it determines if an actinide is present and whether it is a bomb.

SmartScan works like this: Trucks leaving the port with cargo are conveyed through a 176-foot tunnel. **The cargo is inspected using high-resolution x-rays and other passive radiation detection methods with proprietary technologies.** Three-dimensional images based on the effective atomic number and density are generated as the system measures photon signals to determine anomalies, such as explosives or radioactive material. Additional technology determines if special nuclear materials are present.

Acknowledging reality: A pragmatic approach to Pyongyang

By Shen Dingli

Source: http://thebulletin.org/north-koreas-nuclear-weapons-what-now

June 01 – **With North Korea having conducted its fourth nuclear test in January, the Korean Peninsula seems more distant than ever from denuclearization. Given this reality, what's the most effective way to approach the nuclear problem?**

The obstacles to progress are enormous. Pyongyang's inclinations are strongly realist, and the country's leadership sees nuclear deterrence as the ultimate guarantee of security. It will likely continue to see things that way for some time. The North perceives Washington's attitude as essentially realist as well—so Pyongyang is likely betting that US policy toward North Korea will eventually change direction. This is especially true considering that Washington experiences regime change every four or eight years.

The North may in fact believe that Washington, once it accepts the nuclear reality on the Korean Peninsula, will ease sanctions. This calculus may make sense. The United States never approved of Israel's possession of nuclear weapons, but it has had to live with the hard reality of a nuclear Israel—and protect Tel Aviv from the establishment of a Middle East nuclear-weapon free zone. Nor does Washington approve of a nuclear India, and indeed it imposed sanctions on New Delhi following India's 1998 nuclear test. But those sanctions were lifted within days of the 9/11 terror attacks. In 2008 the United States even waived its ban on civilian nuclear cooperation with India—a ban it had imposed through the Nuclear Suppliers Group, which it helped create in 1975 precisely to punish India for its "peaceful" nuclear test in 1974. As for Pakistan, the United States designated that country a major non-NATO ally in 2004 in order to gain Islamabad's cooperation in the fight against terrorism—despite Pakistan's development of nuclear weapons. Meanwhile, President Obama is pursuing normalized relations with Cuba after decades of hostility between Washington and Havana. All this may encourage Pyongyang to believe that Washington will not wait additional decades to normalize relations with North Korea.

Meanwhile, China and North Korea have been allies for decades. But China has been cooperating more closely with the United States on sanctions against North Korea, so Pyongyang likely feels betrayed

by Beijing. Then again, considering the rising distrust that characterizes Washington and Beijing's relationship, the North may be betting that China will hedge against any future possibility of US reconciliation with the North.

North Korea has certainly noted China's insistence that sanctions against Pyongyang must not generate instability on the Peninsula, risk war, or create humanitarian problems. China is simply unwilling, whether Pyongyang has nuclear weapons or not, to see North Korea collapse. This stance would seem to ensure North Korea's survival. In fact, Beijing may be more concerned about Washington's "rebalancing" in Asia than it is about Pyongyang's nuclear program. Beijing and Washington may cooperate on North Korea to some degree, but they don't trust each other, and both sides will hedge their bets. This could well play into North Korea's hands, and compromise the effectiveness of US-China collaboration.

Consequently, the Korean Peninsula won't likely be free of nuclear weapons any time soon. So any successful approach to the Korean nuclear issue must be incremental, pragmatic, and cooperative in nature; and must provide assurances to all sides. North Korea will only be enticed by denuclearization proposals that espouse a win-win philosophy.

What might be workable, on an interim basis, is to demand of North Korea a "three noes" policy: no further development of nuclear weapons (including nuclear tests); no transfers of nuclear weapons outside North Korean territory; and no using (or threatening to use) nuclear weapons. Essentially, Pyongyang would be asked to accept a "nuclear freeze" regime—which would include a unilateral arms control ceiling and an appropriate verification system. In return, North Korea would receive a package of benefits including a multilateral security assurance arrangement; initiation of a diplomatic process toward normalization of North Korea's relations with the United States and other nations; and removal of economic, trade, and investment sanctions—if Pyongyang adheres to the "three noes."

Clearly, such a process wouldn't achieve denuclearization at once. But North Korea is adamant about not relinquishing its nuclear capabilities, so any path toward disarmament must be phased. Establishing denuclearization as a short-term objective would only invite total failure. It's better just to get the ball rolling with diplomacy.

Essentially, the goal of the "three noes" would be to establish a productive atmosphere of cooperative nuclear restraint. In some ways, this formula resembles the approach underlying the Iran nuclear deal. In negotiations toward that deal, the international community could not prevail on Iran to accept complete, verifiable, and irreversible dismantlement of its nuclear programs. But Iran *did* commit itself to eliminating the lion's share of its uranium enrichment capacity—though it nonetheless retains certain nuclear fuel cycle competencies. The point is that both sides compromised: Iran obtained sanctions relief by curtailing its dubious nuclear operations, while the international community greatly reduced the risk that Iran will become a nuclear weapon state, even if complete dismantlement wasn't achievable.

If this model were followed on the Korean Peninsula—if nuclear tensions were contained through cooperative, incremental measures aimed at nuclear threat reduction—the international community (North Korea included) could reinvigorate a diplomatic process toward a nuclear-free Korean Peninsula. Once the initial stages of the approach succeeded, Pyongyang's leadership might transform its outlook toward the importance of nuclear arms in national security. Eventually the North might be ready to take concrete steps toward eliminating its entire nuclear arsenal.

Denuclearizing the Korean Peninsula is a distant prospect. Such a prospect draws no closer as long as the world rejects pragmatic engagement with the North.

Shen Dingli *is a professor and associate dean at Fudan University's Institute of International Studies in Shanghai, China. He has taught international security and China-US relations in both China and the United States. His research interests include nonproliferation, regional security, and the foreign and defense policies of China and the United States. He is vice president of the Chinese Association for South Asian Studies and of the Shanghai Association of International Studies. He received his doctorate in physics from Fudan University in 1989 and did postdoctoral work in arms control*

at Princeton University from 1989 to 1991. He was an Eisenhower Fellow in 1997 and belongs to the Global Council of the Asia Society.

How will the United States upgrade its nuclear weapons arsenal?

Source: https://us-mg6.mail.yahoo.com/neo/launch

July 31 – **Advancing the United States's commitment to modernizing its aging nuclear fleet, the Air Force put out the call Friday for industry proposals to redesign its air-launched nuclear cruise missile and land-based intercontinental ballistic missile (ICBM) system.**

The two projects fall within the government's efforts to upgrade the country's nuclear arsenal, at an estimated cost of $1 trillion over three decades and reignite a longstanding debate about whether the United States needs to maintain each of the three legs in the triad of its nuclear deterrence strategy, with warheads poised to launch from land, sea, and air, even with a much smaller total arsenal.

The need to update the US nuclear arsenal is broadly acknowledged, but while some experts advocate preserving the triad, others argue for focusing on the most effective weapons.

The Air Force said in a statement it will award two contracts for a new ICBM system by the end of 2017, to replace the Minuteman III missile, whose launch systems and physical infrastructure have been updated over the years but date back to the mid-1960s. Military contractors Boeing, Northrop Grumman, and Lockheed Martin will also compete to design the new air-launched missile to replace a weapon from the 1980s that has a 10 year design life.

In part, "This request for proposals is the next step to ensuring the nation's ICBM leg of the nuclear triad remains safe, secure and effective," said Major General Scott Jansson, who leads the Air Force program office for strategic systems. The request will also help build up the air-launched leg of the triad.

Some critics say that the US no longer needs ICBMs. "We have ample deterrence from the submarine force, and certainly if you add the bomber force to that, that's an overwhelming deterrence force. So I cannot understand the argument that we also need ICBMs for deterrence. We might need ICBMs for other reasons, for geopolitical reasons, but not for deterrence. Any sane nation would be deterred by the incredible striking power of our submarine force," Former Defense Secretary William Perry (and author of the book My Journey at the Nuclear Brink) said during an interview with the Arms Control Association.

Similarly, Nikolai Sokov, senior fellow at Center for Nonproliferation Studies in Monterey, claims that it would make sense to seriously consider moving from the nuclear triad to a two-component dyad, asking, "Does it really make sense to spend all the money on a new land-based missile, when the addition to the overall force is limited?"

US standards and planning around nuclear weapons have not been sufficiently updated since the Cold War, Dr. Sokov argues.

"The smaller the force, the more thought you need to give to the composition of the force. I would say that the Cold War standards of how you plan the force no longer apply. During the Cold War, we had thousands upon thousands of nuclear weapons. I'm just not really sure that anyone seriously considers the technical and financial impact of a much smaller force."

The US stockpile of nuclear weapons has declined from 19,008 warheads at the collapse of the Soviet Union in 1991 to 4,571 in 2015, according to the

Defense Department. Today, the strategic arsenal hovers around 1,500 deployed warheads. Russia's President Vladimir Putin has refused President Obama's overtures for a bilateral agreement to drop that number even further to 1,000.

Despite these calls to cut some of the weapons, other expert think that it makes sense to maintain all legs of the nuclear triad. "If we go ahead and make the investments, you basically decrease the chance of a nuclear and even a conventional war," says Richard Weitz, Director & Senior Fellow at the Center for Political-Military Analysis of the Hudson Institute.

The idea behind updating each of the three legs, which have served the US since the 1950s, is to account for the strengths and weaknesses of each.

"They have different pluses and minuses. They complicate the ability of any opponent to basically neutralize the nuclear arsenal," says Dr. Weitz. "Generally it's been thought that it's worth having all three legs and that's my belief as well."

The land-based nuclear missiles can be launched quickly, carry a lot of warheads, and are extremely accurate, but they can be targeted by US adversaries because they're stored in silos whose location is known. The advantage of submarines is that they're mobile, so no one knows where they are, but problems arise if they were to be detected or lose contact with their land-based commander. The effectiveness of the strategic bombers has declined over the years, as air defense systems have become more sophisticated.

There is a logic to retaining as many different kinds of nuclear weapons as the US can afford. "The Russians and the Chinese and even the Iranians – a lot of countries are building much better defenses against air missile attacks. You'd want to keep the bombers as far away from the anti-air defense as possible, and you'd want to make sure the missiles you launch are able to evade them as well. So basically that is the problem. The air defenses have made a lot of progress throughout the world, so it's a lot harder for a bomber to approach and attack a target," Dr. Weitz says.

Despite the debate among experts, the Air Force is moving ahead with its plans to modernize its land-based and air-based nuclear deterrent. "The main concern is long-term and these systems will last for decades. We wanted to have Russia as a partner at the end of the Cold War and that hasn't happened and it's unlikely to happen anytime soon, so we need to have the nuclear deterrent," Dr. Weitz says.

In memory

71st anniversary of Hiroshima Nuclear Holocaust (Aug 6, 1945)

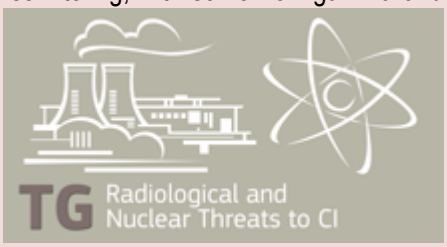
Radiological and Nuclear Threats to Critical Infrastructure

Source: https://erncip-project.jrc.ec.europa.eu/networks/tgs/nuclear

JOINT RESEARCH CENTRE
European Reference Network for Critical Infrastructure Protection (ERNCIP)

The Thematic Group focusses on the following three current areas:

- List-mode data acquisition based on digital electronics. Time-stamped list-mode data format produces significant added value compared to more conventional spectrum format. It improves source localisation, allows signal-to-noise optimisation, noise filtering, with some new gamma and neutron detectors requiring list-mode to function. List-mode approach also allows precise time synchronisation of multiple detectors enabling, for example, simultaneous singles and coincidence spectrometry such as singles gamma and UV-gated gamma spectrometry.



- Remote-controlled radiation measurements and sampling using unmanned vehicles. There are several measurement and sampling scenarios that are too risky for humans to carry out. Applications envisaged are: reactor and other accidents, dirty bombs before and after explosion, search of sources out of regulatory control etc
- Expert support of field teams, i.e. data moves instead of people and samples. Fast and high quality response can be achieved with less people. Optimal formats and protocols for reach-back.

Main achievements

In response to the report delivered by CEN/TC 391 "Societal and Citizen Security" to the Commission in the frame of mandate M/487 "security standards", DG HOME entrusted JRC-ERNCIP with the objective to develop a report/draft standard that includes the basic elements concerning the list-mode data format based on digital nuclear electronics, for consideration by the appropriate standardisation community.
In 2014, the ERNCIP RN Thematic Group published two reports discussing the current state-of-the-art and critical parameters of digital data acquisition hardware, and proposing the first elements of a standard (EUR 26715; EUR 26976). In 2015, a survey was conducted to assess the needs of end-users, to be taken into account in the development of a preliminary draft standard. The ERNCIP RN Thematic Group triggered the establishment of a consortium of Member States laboratories who receive H2020 funding through Euramet for the development of an accepted committee draft. The consortium partners are NPL (UK), STUK (Finland), ENEA (Italy) and CEA (France). JRC takes part as an unfunded partner.
On 15 October 2015, and in agreement with the consortium, JRC submitted to IEC/TC 45 a New Work Item Proposal, accompanied by a preliminary draft, for the development of the new standard. The proposal was accepted by the IEC/TC 45 National Committees.
The envisaged publication date of the standard IEC 63047 is March 2019.

In dirty bomb prevention, Texas fails a crucial test

By Patrick Malone

Source: http://www.homelandsecuritynewswire.com/dr20160805-in-dirty-bomb-prevention-texas-fails-a-crucial-test

Aug 05 – **The clandestine group's goal was clear: Obtain the building blocks of a radioactive "dirty bomb" — capable of poisoning a major city for a year or more — by openly purchasing the raw ingredients from authorized sellers inside the United States.**

It should have been hard. The purchase of lethal radioactive materials — even modestly dangerous ones — requires a license from the Nuclear Regulatory Commission, a measure meant to keep them away from terrorists. Applicants must demonstrate they have a legitimate need and understand the NRC's safety standards, and pass an on-site inspection of their equipment and storage.

But this secret group of fewer than ten people — formed in April 2014 in North Dakota, Texas, and Michigan — discovered that getting a license and then ordering enough materials to make a dirty bomb was strikingly simple in one of their three tries. Sellers were preparing shipments that together were enough to poison a city center when the operation was shut down.

The team's members could have been anyone — a terrorist outfit, emissaries of a rival government, domestic extremists. In fact, they were undercover bureaucrats with the investigative arm of Congress. **And they had pulled off the same stunt nine years before.** Their fresh success has set off new alarms among some lawmakers and officials in Washington about risks that terrorists inside the United States could undertake a dirty bomb attack.

Here's how they did it:

In Dallas, they incorporated a shell company they never intended to run and rented office space in a nondescript industrial park, merely to create an address for the license application. In a spot on the form where they were supposed to identify their safety officer, they made up a name and attached a fake résumé. **They claimed to need the material to power an industrial gauge used in oil and gas exploration.**

Last year, their application was sent not to Washington but to Texas regulators, who had been deputized by the NRC to grant licenses without federal review. **When the state's inspector visited the fake office, he saw it was empty and had no security precautions.** But members of the group assured him that once they had a license, they would be able to make the security and safety improvements.

So the inspector, who always carried licenses with him, handed them one on the spot.

The two-page Texas document authorized the company to buy the sealed radioactive material in an amount smaller than needed for any nefarious purpose. But no copies were required to be kept in a readily-accessible, government database. **So after using the license to place one order, the team simply made a digital copy and changed the permitted quantities, enabling it to place a new order with another seller for twice the original amount**.

"I wouldn't call what we did very sophisticated," Ned Woodward, the mastermind of the Government Accountability Office's plot, said in a phone interview with the Center for Public Integrity. "There was nothing we had done to improve that site to make it appear as if it were an ongoing business."

In 2007, Woodward's colleagues in the GAO similarly set up fake businesses, got licenses to purchase low-level radioactive material and altered them to buy larger quantities. The NRC promised "immediate action to address the weaknesses we identified," according to the GAO's report on that incident.The auditors' aim this time around was to see whether the government had cleaned up its act and taken steps to close some simple gateways to obtaining the ingredients for a dirty bomb.

It turns out, the government had not.

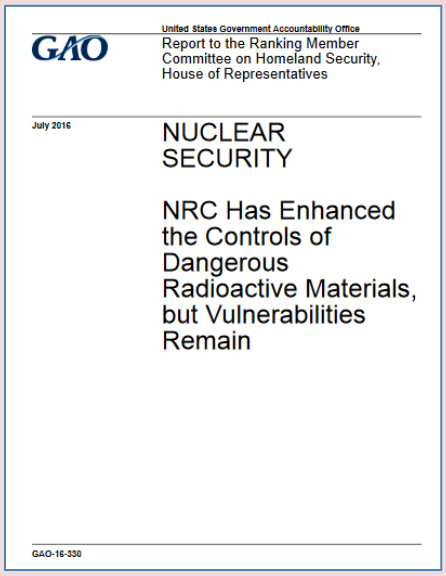
While the purchases that Woodward's team set in motion were never completed, if they had been, his group would have had enough radioactive material to create the type of dangerous dirty bomb that terrorists may seek, according to David Trimble, director of Natural Resources and Environment at the GAO and Woodward's boss. It would have been within the group's reach to spread cancer-causing americium and beryllium dust over many blocks, threatening the health of anyone who breathed it.

The quantity each seller could have sent was dangerous, and together the quantity was "significantly dangerous," Trimble said, speaking on a GAO podcast. He said he is confident his investigators could have altered the license again and again, allowing them to amass an even larger quantity. "It's a back door," he said in an interview. "We

walked through it and we showed the door was still open. We could have kept doing it. If you can forge [a license] once, there's no reason you can't forge it again and again."

Texas nuclear regulatory officials have responded by quietly firing two managers and organizing new training efforts. NRC Commissioner Jeff Baran, a lawyer and former House staff member, wrote a swift letter to the two other current NRC commissioners (two positions are vacant) stating that even if Texas changed its procedures, "GAO's covert testing identified a regulatory gap." He urged his colleagues to consider creating a system for tracking licenses and sales of low-level radioactive materials — an idea that its members rejected seven years ago under heavy state and industry pressure.

The GAO's 15 July report on the episode, which described the bare bones of its scam without naming any of the states involved or identifying the precise materials that were improperly ordered, similarly said that the NRC and state regulators aren't doing enough to keep such materials out of terrorists' hands. It criticized the state regulator for granting the licenses, but also said the commission needs to act to block license alterations and track sales and shipments of lower-level radiological materials, using measures like those already in place for the sale of more hazardous fissile materials.


United States Government Accountability Office
GAO
Report to the Ranking Member Committee on Homeland Security, House of Representatives
July 2016
NUCLEAR SECURITY
NRC Has Enhanced the Controls of Dangerous Radioactive Materials, but Vulnerabilities Remain
GAO-16-330

Billions of dollars in potential economic harm

Unlike a nuclear detonation, which could destroy a large city, the explosion of a dirty bomb would provoke more chaos than immediate fatalities, according to a 2007 study commissioned by the Department of Homeland Security.

"A terrorist attack using a dirty bomb in the United States is possible, perhaps even moderately likely, but would not kill many people," two professors at the University of Southern California wrote in the study, which was conducted with advice from government scientific and counterintelligence experts. "Instead, such an attack primarily would result in economic and psychological consequences."

The explosion could be lethal to someone nearby or to the first emergency personnel to arrive. But cleaning up the contaminated area would cost billions of dollars and take about a year in the scenario examined by the study's authors — a dirty bomb targeting the ports of Los Angeles and Long Beach, which together constitute the third-busiest in the world. At its worst, the resulting economic harm could exceed $250 billion.

One key to keeping the ingredients out of terrorists' hands, the authors concluded, is "being more proactive in controlling and protecting the original sources of radioactive material." But they also warned that "an attack that involves relatively low-level radioactive material from a U.S. facility" — the precise scenario tested by the GAO — is more likely to be successful than an attack using imported material, because the chances of detection are so much less.

"Why bother smuggling it if you can just order it with a fake license," Trimble said.

Radioactive materials considered useful in a dirty bomb are widely present in U.S. and international commerce, used legitimately for **medical and industrial purposes in more than 70,000 high-risk devices located at 13,000 buildings, according to a 2013 Energy Department estimate**. These include machinery that irradiates food or blood products or is used to diagnose illness. **In the United States alone, about 21,000 licenses for the purchase of these materials are active — and in some states they are reviewed by regulators only once a decade.**

The Obama administration highlighted the dangers associated with loose radioactive materials at international summits in 2010, 2012, 2014 and this March. On March 31, President Obama's deputy national security adviser Ben Rhodes warned reporters at a media briefing that while terrorists would have a hard time building or stealing a working nuclear weapon and delivering it, making a "more rudimentary dirty bomb" would be less challenging.

Coordinated suicide bombings in Brussels nine days earlier had stoked special anxiety about dirty

bombs, because two perpetrators had secretly surveilled a senior researcher in a Belgian radioactive isotope program as he came and went from his home. The resulting videos, which police seized, prompted worries that the terrorists wanted to kidnap the man to force a handover of radioactive materials. The Belgian video suggested that "terrorist organizations like al-Qaeda and ISIL have an interest in getting their hands on these types of materials," Rhodes said at the summit media briefing, using an acronym for the Islamic State. "They want to do as much damage as possible. That was al-Qaeda's position for many years; we have no reason to doubt that that is ISIL's position as well."

The Obama administration's ambition in convening the summits, Rhodes said, was to "bring the standard up around the world so that it is at the level that we see certainly here in the United States."

That level, it turns out, isn't so high.

Tighter regulation rejected in 2009

In a written statement about the report, Rep. Bennie Thompson, D-Miss., the ranking Democrat on the House Committee on Homeland Security, who asked for the GAO's investigation, said, "radiological and nuclear terrorism remains a threat to our nation's security," and the GAO's scam showed how easy it is to exploit gaps in the NRC's oversight that should have been fixed years ago.

"The NRC should re-evaluate its licensing requirements to ensure those who want to do us harm cannot obtain a license to purchase radioactive materials as easily as covert testers did," Thompson said.

Similar demands were made, but refused, after the GAO's sting operation in 2007 exposed the same weaknesses. Then, NRC staff proposed requiring that all licensing and sales involving "Category 3 radioactive materials" — those in types or quantities considered less dangerous than others — be tracked in a single national database, as they already were for higher-risk Category 1 and 2 materials. Otherwise, it said, these Category 3 materials might be accumulated surreptitiously — through the process the GAO used — "for potential malevolent use."

Companies that sell radiological materials complained in response that they couldn't even begin to guess how burdensome an expanded tracking system might be for them. Regulators in 24 of the states that had been deputized by the NRC to issue licenses also registered their opposition to the expanded tracking, partly because the system for tracking more dangerous quantities was then not working well.

Only Minnesota supported the proposal, calling it one of several "essential steps" that were "long overdue." Then-NRC member Peter Lyons, a former official at the Los Alamos weapons laboratory, similarly argued at the time that expanded tracking "will further reduce the potential for aggregating sources" to a dangerous level. But NRC Commissioner Kristine Svinicki, a nuclear engineer who had worked on the civilian side of the Energy Department, said she thought the on-site inspections would be enough to stop thefts or diversions.

In June 2009, the radioactive material sellers and state regulators got their way. The NRC rejected on the plan with a 2-to-2 tie vote.

That left in place regulations for keeping low-level radioactive materials out of terrorists' hands that were written in 1978. While the NRC is technically responsible for overseeing these rules, in practice it has granted only 13 percent of the active purchase licenses, relying instead on inspectors in 37 states to oversee the rest. They are supposed to get NRC training, and to follow the NRC's 14-point checklist rules for inspections. This is what the GAO sought to verify: "We designed our test to fail" through egregious behavior during on-site visits, the report said.

The NRC had previously judged North Dakota's on-site inspections deficient. With high staff turnover fueled by higher-paying jobs in the state's booming oil and gas industry, the NRC decided in 2011 to put its radiation protection office into a remedial "heightened oversight" program. But the GAO's experiment failed there, showing the state had turned around. The applicants' facility was unsuited for the kind of work they said they intended to do. They "couldn't even get a well-logging truck through the door of this building they'd rented," said Dale Patrick, manager of the radiation program at the North Dakota Department of Health, in a telephone interview.

Similar concerns arose during a second GAO licensing effort in Michigan, where NRC regional inspectors from Illinois also blocked the GAO's scam.

But Texas failed the GAO's test last year because its inspector didn't follow agreed procedures "to make sure this unknown entity was a legitimate company and did not question that the applicant was not a registered business with the Texas secretary of state," according to Christine Mann, a spokeswoman for the Texas Department of State Health Services.

Texas's on-site inspectors routinely carried licenses with them and commonly handed them to applicants on the spot without consulting anyone else about what they'd observed. The practice meant that a single person, operating in the field and without independent scrutiny, functioned as the sole obstruction to improper sales.

"Yes, that did happen, but we no longer allow that to occur," Mann said.

The GAO's sting spurred change in Texas. The state fired two managers and sent letters of reprimand to two members of its licensing staff, according to Mann. The radiation control department retrained its personnel, and altered its procedures to require supervisory reviews of all licenses. A new NRC review in February, however, noted that the division still had "budgetary shortfalls" because the state was using its regulatory fees to raise revenues that it then spent for other purposes. It had 42 personnel to oversee more than 1,570 licensees and shippers and thousands of transactions each year.

After being briefed by the GAO on what had happened, the NRC immediately revoked the license Texas had granted the GAO's shell company and told the vendors to cancel the orders. The NRC also asked all its state-level partners and regional NRC offices to review their licensing practices and updated its training courses to emphasize the need for heightened scrutiny. But unnamed NRC officials told the GAO that **"NRC had no current plans to take action" to enact stricter regulations, because the issue had been considered and rejected in 2009.**

After the report's release, however, Duncan White, a senior health physicist at the NRC, wrote in an official blog post that NRC staff will restudy the issue and discuss it further with the commission later this year.

"We're encouraged that NRC appears to be looking closely at this issue and considering the merits of the recommendation that we made," Trimble said, "which we believe is on point."

***Patrick Malone** is a reporter for the Center for Public Integrity, a nonprofit, nonpartisan investigative media organization in Washington, D.C.*

EDITOR'S COMMENT: I am struggling to find something nasty to write herin but nobody on Earth can comment on stupidity and universe (other than Einstein). But when people" are unable or unwilling to learn then it is the duty of state to "decapitate" the sick chain of command – ALL of them; not just two employees! In that repect, the newcomers will think twice (at least) when going into their office in the morning! If not, soon new employees will be "absorbed" by their dysfunctional environment and dublicate mistakes of the past. Eagerly waiting for the next GAO report with the new "red team" adventures! (or perhaps a Hollywood movie based on this scenario)

UVA Researchers Identify Potential Countermeasures for Radiation Exposure

Source: http://globalbiodefense.com/2016/06/02/uva-researchers-identify-potential-countermeasures-radiation-exposure/

June 02 – **University of Virginia School of Medicine researchers have identified promising drugs that could lead to the first antidote for radiation exposure that might result from a dirty bomb terror attack or a nuclear accident such as Fukushima.**

Currently there is no treatment for people exposed to lethal doses of radiation; doctors can only try to ease their suffering until death. "If you're exposed to a very, very high dose, it's rapid deterioration and immediate death," explained John S. Lazo, PhD, of UVA's Department of Pharmacology. "It's the lower doses that people – particularly governments – are concerned about. The type of

exposure that might result from a dirty bomb or a nuclear accident. How do we alleviate the effects? What's the antidote? Right now, we just don't have anything."

Lazo and his colleague Elizabeth R. Sharlow, PhD, screened a library of more than 3,400 existing drugs, vitamins and other compounds to identify ones that might help cells withstand the effects of radiation exposure. The goal was to keep stem cells – the cells that produce the various cell types in the body – alive long enough to repair the damage caused by radiation.

Some of the compounds, including the drug rapamycin, have previously been shown to extend life in organisms such as worms and flies, though it's unknown if they would have the same benefit in humans. UVA's research suggests that these compounds, or similar drugs, might counter the deadly effects of ionizing radiation.

"We wanted to find already approved drugs that would potentially keep stem cells, or progenitor cells, alive after radiation exposure," Sharlow said. "That's very much of interest to the NIH right now: How can we keep those self-renewing populations alive so they can actually help heal the effects of radiation exposure?"

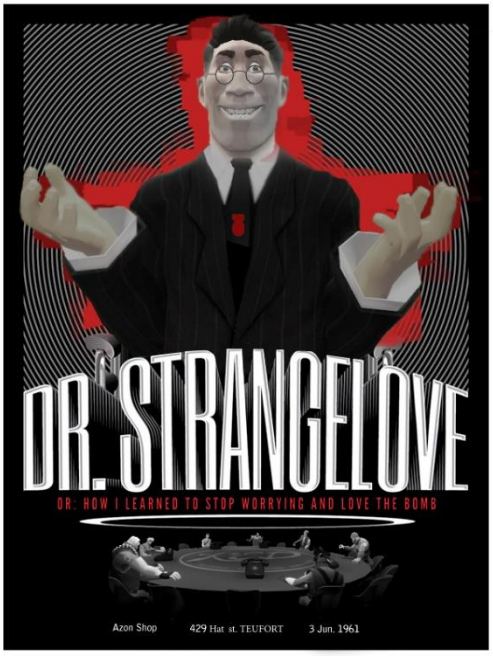
After they identified potential leads, Sharlow created 3D computer models to compare the substances' chemical structures. That analysis identified a cluster of promising compounds with similar structures – a tantalizing lead in the quest for an antidote. "If you're a drug hunter, the way we are, this is really cool information," Lazo said. "Because you can say, 'Now I will look in the universe of 40 million compounds. What else looks like that? Are they useful?'"

He noted that it is unlikely any one drug or compound will work on its own. "A lot of us in this field think it will be a cocktail of things you take," he said. "And if you think you need cocktails, you need the individual ingredients. That's why we think this is pretty important – because it's providing new ingredients for that cocktail."

▶ **Read the paper:** *A Small Molecule Screen Exposes mTOR Signaling Pathway Involvement in Radiation-Induced Apoptosis*

Why Trump's potential access to nuclear weapons has 50 Republican national security experts terrified

Source: http://www.independent.co.uk/voices/donald-trump-republican-party-nuclear-weapons-terrified-national-security-experts-quite-rightly-a7180841.html



Aug 09 – Henry Kissinger was said to have been hurt by reports that the film character Dr Strangelove, the swivel-eyed Teutonic accented proponent of America carrying out a nuclear strike, was based on him. Stanley Kubrick, the director of the masterpiece, attempted to mollify President Nixon's hawkish secretary of state by saying that it was an amalgam of Hitler's scientists who had been spirited to the US from Germany after the Second World War.

"Dr Strangelove or How I Learned to Stop Worrying and Love the Bomb", to give the film its full title, was released in 1964. In 1989 The United States Library of Congress picked the black comedy about the Cold War as one of a select group of works for preservation in the National Film Registry. On 6 August, 2016, the world marked the 71st anniversary of the day that America became the first and only nation to use the Atomic bomb, dropping it on Hiroshima.

In just three months, America will be voting in an election in which the Republican candidate, Donald Trump, has held, more than once, that using nuclear weapons is a viable option in a political crisis.

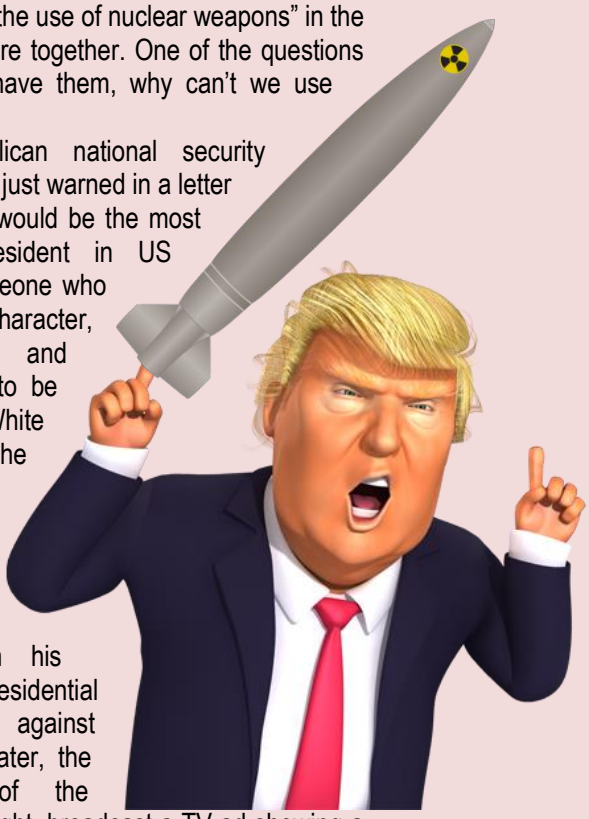
Trump's statements on nuclear strike have been overshadowed by all the other extraordinary things he had said in his extraordinary campaign. But the fact remains that the man who may yet become the world's most powerful head of state has been asking why America's military commanders have not used their nuclear weapons of mass destruction since Japan.

In an interview with MSNBC last March, asked about nuclear strikes, Trump responded "Somebody hits us within Isis, you wouldn't fight back with a nuke?" He refused to rule out using nuclear weapons in Europe, saying "Europe is a big place, I'm not going to take my cards off the table". Defence strategists who have been called in to advise the Republican candidate say he is genuinely puzzled why using the bomb is not more part of current combat doctrine. He wants to be "unpredictable" about what he may or may not do with nuclear weaponry.

Perhaps the special relationship Trump wants to forge with Vladimir Putin and his warning that he may not act to protect the Baltic states from any future Russian aggression will mean that an American nuclear strike will not be necessary in Europe. But Trump also appeared to be ignorant of the history of deterrence and, while he has, like other right-wing Republicans, castigated Barack Obama over the Iran nuclear deal, he seems sanguine about nuclear proliferation, saying that he would have no problem with Saudi Arabia, South Korea or Japan getting the bomb.

Trump holds that nuclear weapons and the ramification of their use is a pretty simple matter. "It would take an hour and half to learn everything there is to learn about missiles...I think I know most of it anyway," he has declared. Hilary Clinton has, naturally taken advantage of all this. She asked voters to "Imagine him in the Oval Office facing a real crisis. A man you can bait with a tweet is not a man we can trust with nuclear weapons."

But it was a conservative Republican talk-show host, Joe Scarborough, who has been among the first to raise the issue and express his concern. It was he who revealed that a foreign policy expert giving Trump a national security briefing had been disturbed that "three times he asked about the use of nuclear weapons" in the hour they were together. One of the questions was "if we have them, why can't we use them?"



Fifty Republican national security experts have just warned in a letter that Trump "would be the most reckless president in US history", someone who "lacks the character, values and experience" to be in the White House. The Republicans will remember how Lyndon Johnson, in his 1964 presidential campaign against Barry Goldwater, the candidate of the Republican right, broadcast a TV ad showing a little girl counting flower petals as mushroom cloud envelops the screen. The ad was shown just once, but was seen as having a major impact in securing Lyndon Johnson's victory.

Henry Kissinger, whose name was not on the letter condemning Trump, apparently never fully accepted that Dr Strangelove, who was played by Peter Sellars, was not, at least partly, based on him. Sellars also played the part of the US president, Merkin Muffley in the film. At first he made the character a comic one, but then decided that was inappropriate. The leader of the 'free world' should be portrayed, he decided after speaking to others, as a "responsible and stable character" in the drama.

In his show, Joe Scarborough had recently asked former CIA director Michael Hayden, one of the signatories of the Republican letter, whether there were checks and balances to ensure that if Trump "gets angry, he can't launch a launch a nuclear weapon", given the perception that he might not be "the most stable guy". Hayden replied "The system is designed for speed and decisiveness, it's not designed to debate the decision. He is inconsistent, and when you're the head of a global super power,

inconsistency, unpredictability are dangerous things. They frighten your friends and they tempt your enemies. And so, I would be very concerned."

Innovative Approaches to Radiological/Nuclear Preparedness

By Erin Mohres & Darren Chen

Source:http://www.domesticpreparedness.com/First_Responder/Emergency_Management/Innovative_Approaches_to_Radiological-!Nuclear_Preparedness/

Aug 10 – In 2013, truck drivers were stopped at a gas station along the highway in Mexico when they were assaulted, and their truck was stolen. Unknown to the thieves, the truck was transporting a teletherapy machine for treating cancer, from a hospital in Tijuana to a waste-disposal site. The machine contained a Category 1 cobalt-60 source. Mexican authorities began a search and reported the theft to the International Atomic Energy Agency (IAEA). The radiological source was located days later in a nearby field; the capsule holding the source had not been opened, but it had been removed from its protective shielding. The strength of the cobalt-60 was reported to be 3,000 curies, strong enough to kill a person directly exposed to it. In this case, the thieves were located and determined not to have received dangerous exposure levels. The truck thieves in Mexico most likely had left behind the device after learning more about their stolen item, either from the warning labels or local news reports.

In the United States, public safety practitioners typically agree that consequences will be severe after an improvised nuclear device (IND) detonation, or even after a radiological dispersal device (RDD) detonation, but there is often skepticism about the likelihood of the threat. Such skepticism poses challenges to state and local preparedness efforts. Increased awareness about IND/RDD threat and other radiological/nuclear-related incidents, as well as the pursuit of some innovative approaches to preparedness, may shed light on this often-overlooked set of threats.

The Threat

Legal sources of radiation that go missing. Legal, regulated radiological sources are more abundant than many realize. Radiological sources in medicine often use cobalt-60, cesium-137, or iridium-192. Major construction sites, research universities, and agricultural sites may also use sources of radiation, such as nuclear gauges, irradiators, and even reactors. In the United States, such sources are regulated by the Nuclear Regulatory Commission (as defined in the IAEA's Code of Conduct, Categories 1-5), based on their potential risk to human health if not managed appropriately.

Licensed radiological sources typically have specific security measures in place, but lost, stolen, or orphaned sources can be used in ways they were not originally intended, or can accidentally cause unintended consequences. Member countries voluntarily report thefts to the IAEA. Although such thefts are relatively rare (especially thefts of Category 1 sources), these thefts do not need to be prevalent to warrant prevention and protection measures.

Intentional exposure. A former agent of Russia's KGB and its successor organization, the Federal Security Service, was granted asylum in the United Kingdom in 2000. He was a vocal critic of the Kremlin. In 2006, he suddenly became ill and entered a London hospital. His health steadily declined, and he died several weeks later. An investigation determined he had been poisoned by polonium-120, likely via a cup of tea. Traces of this radioactive material were discovered in London, Germany, Russia, and on passenger jets, resulting in hundreds of people needing (or wanting) to be tested.

This event has been unique in history, but its response required extensive public safety and medical resources from London authorities, including police to conduct searches and seal off a series of both public and private sites where radioactivity was found, forensics scientists to conduct sampling and testing, and public health and medical staff to test potentially exposed residents.

Insider threat. Simple online searches reveal a number of cases of insider threat in radiological/nuclear (rad/nuc) industries around the world, dating back to the 1970s, all of which could have had significant consequences. As both the threat itself and mitigation measures to combat such threats have evolved over time, a recent case at Los Alamos Plutonium Facility is interesting in its simplicity. In

March 2009, a technician at the plant attempted to steal two ounces of gold used in research, which was worth approximately $2,000. The gold was contaminated with plutonium, and even though the technician attempted to decontaminate it, he set off a radiation portal monitor when trying to leave the plant. Had this attempted theft been successful, it could have posed a health threat to members of the public and required both a public safety and public health response. Fortunately, measures and processes were in place at this plant that prevented the successful theft.

Insider threat has become high profile in recent years. In fact, one of the outcomes of the 2016 Nuclear Security Summit that took place in April in Washington, D.C., was the Joint Statement on Insider Threat Mitigation, outlining a number of activities numerous countries will take "to establish and implement national-level measures to mitigate the insider threat." The case studies above are simply a sample of some of the types of rad/nuc threat that may be faced by state and local authorities in the United States. Next, resources are described that may offer state and local government officials additional information on rad/nuc-related threat information.

Preparing for Rad/Nuc Events

In attempting to prepare for rad/nuc events, there is good news: a wealth of robust, technical resources is available to help agencies plan for and respond to such events. The challenge for state and local emergency management agencies is that navigating them and determining how to best incorporate them into local planning efforts is not always easy. It requires dedicated staff, ideally with background knowledge in this area and with sufficient management expertise to leverage existing governance structures and operations in an environment of scarce resources.

Key guidance documents. Literature abounds on rad/nuc topics, and rad/nuc response is a capability of many hazardous materials teams. For planners and emergency managers building new programs, a few sources that may be particularly useful include:

- ***Planning Guidance for Response to a Nuclear Detonation*, 2nd edition, published in June 2010 by the Homeland Security Council Interagency Policy Coordination Subcommittee for Preparedness and Response to Radiological and Nuclear Threats.** This document offers detailed planning information regarding shelter and evacuation, medical care, and population monitoring and decontamination. It organizes information by planning zones, helping emergency managers to understand what to expect and what actions to take within various distances of the nuclear detonation.
- ***Response and Recovery Knowledge Product: Key Planning Factors – For Recovery From a Radiological Terrorism Incident*, published in September 2012 by U.S. Department of Homeland Security (DHS) Science and Technology.** This document offers detailed planning information regarding public health and medical priorities, response operations, and waste management (among others). It also provides a detailed scenario based on a successful RDD detonation, along with narrative, map-based, and graphical information describing expected consequences.
- ***Protective Action Guides and Planning Guidance for Radiological Incidents*, published in March 2013 by the Environmental Protection Agency.** This document offers guidance to federal, state, and local authorities to inform decision-making regarding protective actions for the public, such as the need to evacuate, to shelter-in-place, or to avoid consumption of potentially exposed food and water. It is organized around phases, such as the early or emergency phase (hours to days after the incident), the intermediate phase (weeks to months), and the late or recovery phase (months to years, including site-restoration and cleanup). It takes practical considerations into account while incorporating scientifically based recommendations.

Case studies and modelling tools. Despite real-world rad/nuc emergencies being less prevalent than other threats – for example, natural hazards, or even improvised explosive devices – a few well-documented case studies provide insights and important details into what public safety officials might expect should their jurisdiction experience such a disaster, whether intentional or

accidental. For example, in 1985, a private radiotherapy institute in Goiana, Brazil relocated, but it left behind a cesium-137 teletherapy unit in its old building. The building was subsequently partially demolished. Later, two people searching the site for scrap metal found the unit, took part of it home, tried to dismantle it, and ruptured the source capsule. Parts were then sold to a junkyard, some of which glowed blue in the dark, making it of particular interest to friends and family. After several days of passing this material around, exposed individuals became ill. Investigators identified the problem and its source, but in the end, several people died, and many others were injured, exposed, and evacuated. Over 100,000 people were screened.

Many safety measures have evolved since (and partially due to) this particular case study, which is still an important part of the knowledge base for any planner focusing on rad/nuc incidents. The IAEA prepared an extensive report on this event in 1988 titled, *The Radiological Accident in Goiana*.

In addition to applying case studies, modelling the impacts of rad/nuc events in a particular jurisdiction can provide more-detailed information on consequences that might have to be addressed. This may be beyond the capabilities or resources of many local jurisdictions, therefore, some pre-prepared modelling based on a set of assumptions – for example, a 10-kiloton improvised nuclear explosion – is publically available. In addition, useful, actionable outputs from models and studies such as those conducted by Lawrence Livermore National Laboratory and its staff can be found online.

The Domestic Nuclear Detection Office (DNDO). The volume, scope, and scale of rad/nuc planning and analysis resource material can be overwhelming, especially when an emergency manager is unclear how to judge the credibility of various sources, but help is available. The DNDO is a component of DHS and seeks to prevent nuclear terrorism by continuously improving capabilities to deter, detect, respond to, and attribute attacks, in coordination with domestic and international partners. It understands the enormous challenges faced by state and local agencies regarding rad/nuc threats – including potentially catastrophic consequences, coupled with significant resource constraints – and has invested in innovative approaches to support state and local agencies.

The Threat and Hazard Identification and Risk Assessment

As outlined in DHS's *Comprehensive Preparedness Guide 201* (CPG 201, 2nd edition in August 2013), the *Threat and Hazard Identification and Risk Assessment* (THIRA) is a four-step common risk assessment process that "helps the whole community . . . understand its risks and estimate capability requirements." Typically, states, territories, and major urban areas are required to submit an annual THIRA to the Federal Emergency Management Agency (FEMA), as well as tribes that receive homeland security grant funds. The THIRA may involve complex planning and analysis to be completed, including collection of input from multiple sets of subject matter experts and executive decision-makers.

DNDO identified that this requirement poses an excellent opportunity to support planning and analysis for rad/nuc scenarios. As such, it has developed a guidance document titled, *Assessing the R/N Threat: Guidance to Support the Assessment of Radiological/Nuclear Threats for Inclusion in the THIRA*. This document provides step-by-step instructions and examples to create rad/nuc scenarios and the corresponding core desired outcomes, impacts, targets, and required resources, organized by core capability, per CPG 201. DNDO also offers assistance directly to state and local agencies to explain, expand upon, and customize this guidance.

Fusion Center Support

Acknowledging that actionable rad/nuc threat information can be difficult to acquire, DNDO has engaged in multiple efforts to assist fusion centers and other state and local intelligence groups in accessing relevant real-world rad/nuc threat information and analysis. DNDO worked with the DHS Office of Intelligence and Analysis to prepare the *State/Regional Threat Assessment* report published on 4 September 2015 and is currently developing rad/nuc awareness training and technical assistance that will be available later in 2016.

DNDO maintains the *Radiological/Nuclear Detection Guidance for FEMA Preparedness Grants* and manages the Joint

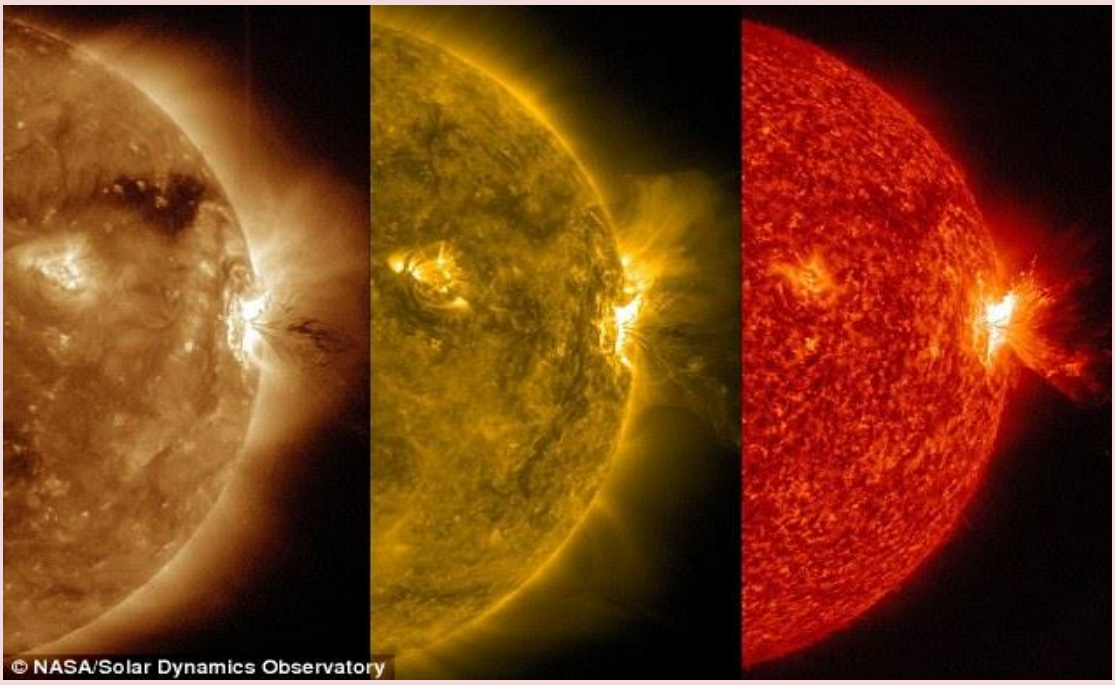
Analysis Center, which provides threat information and products, among other assistance, to state and local partners.

__Erin Mohres__ is a safety and security director with CNA, a nonprofit research and analysis organization. She supports U.S. Department of Homeland Security, Domestic Nuclear Detection Office programs and other federal initiatives focused on state and local emergency management efforts. She was an emergency manager for Miami-Dade County and the City of Fort Lauderdale. She received her MA in International Relations from the University of Miami and her BA in Political Science from the University of Illinois.

__Darren Chen__ is a branch chief with the U.S. Department of Homeland Security, Domestic Nuclear Detection Office, and is responsible for developing national programs supporting state, local, tribal, and territorial radiological/nuclear detection capabilities. He was previously responsible for developing the Department's preparedness grant programs. He received his MA in homeland security and defense from the Naval Postgraduate School, his MS in crisis and emergency management from the George Washington University, and his BA in environmental sciences from the University of Virginia.

1967 solar storm jammed USAF radars, nearly taking U.S. to brink of war

Source: http://www.homelandsecuritynewswire.com/dr20160810-1967-solar-storm-jammed-usaf-radars-nearly-taking-u-s-to-brink-of-war



Aug 10 – **A solar storm that jammed radar and radio communications at the height of the Cold War could have led to a disastrous military conflict if not for the U.S. Air Force's budding efforts to monitor the sun's activity,** a new study finds.

On 23 May 1967, the Air Force prepared aircraft for war, thinking the nation's surveillance radars in polar regions were being jammed by the Soviet Union. Just in time, military space weather forecasters conveyed information about the solar storm's potential to disrupt radar and radio communications. The planes remained on the ground and the United States avoided a potential nuclear weapon exchange with the Soviet Union, according to the new research.

Retired U.S. Air Force officers involved in forecasting and analyzing the storm collectively describe the event publicly for the first time in a new paper accepted for publication in *Space Weather*, a journal of the American Geophysical Union.

The AGU notes that the storm's potential impact on society was largely unknown until these individuals came together to share their stories, said Delores Knipp, a space physicist at the University of Colorado in Boulder and lead author of the new study. Knipp is giving a presentation about the event on 10 August 2016 at the High Altitude Observatory at the National Center for Atmospheric Research in Boulder, Colorado.

The storm is a classic example of how geoscience and space research are essential to U.S. national security, she said.

"Had it not been for the fact that we had invested very early on in solar and geomagnetic storm observations and forecasting, the impact [of the storm] likely would have been much greater," Knipp said. "This was a lesson learned in how important it is to be prepared."

Keeping an eye on the sun

The U.S. military began monitoring solar activity and space weather – disturbances in Earth's magnetic field and upper atmosphere – in the late 1950s. In the 1960s, a new branch of the Air Force's Air Weather Service (AWS) monitored the sun routinely for solar flares – brief intense eruptions of radiation from the sun's atmosphere. Solar flares often lead to electromagnetic disturbances on Earth, known as geomagnetic storms, that can disrupt radio communications and power line transmissions.

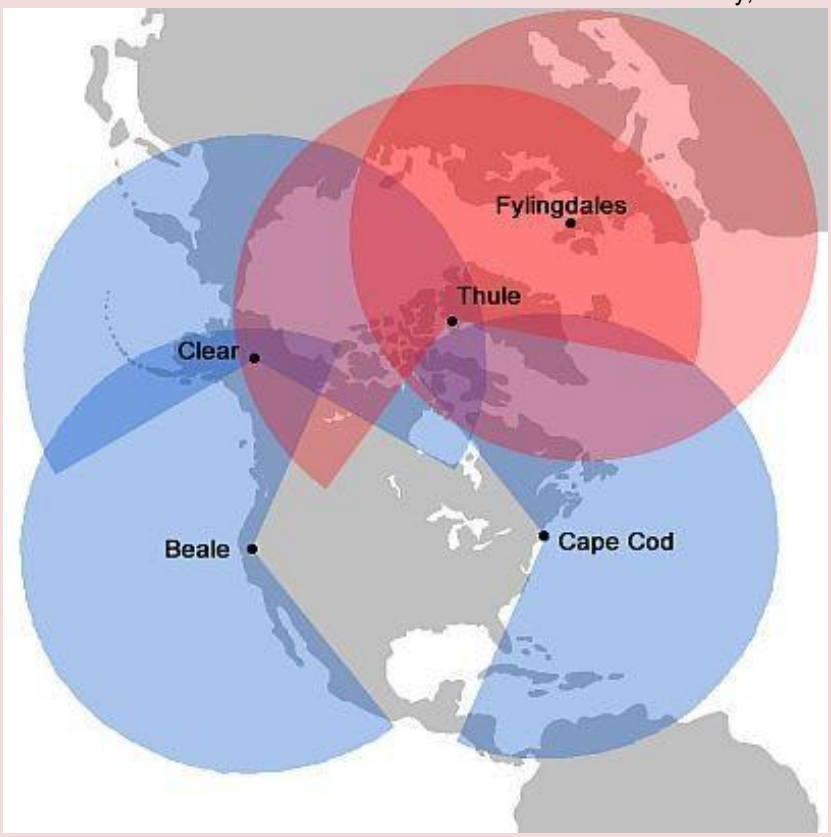
The AWS employed a network of observers at various locations in the United States and abroad who provided regular input to solar forecasters at the North American Aerospace Defense Command (NORAD), a U.S. and Canadian organization that defends and controls airspace above North America. By 1967, several observatories were sending daily information directly to NORAD solar forecasters.

On 18 May 1967, an unusually large group of sunspots with intense magnetic fields appeared in one region of the sun. By 23 May, observers and forecasters saw the sun was active and likely to produce a major flare. Observatories in New Mexico and Colorado saw a flare visible to the naked eye while a solar radio observatory in Massachusetts reported the sun was emitting unprecedented levels of radio waves.

A significant worldwide geomagnetic storm was forecast to occur within 36-48 hours, according to a bulletin from NORAD's Solar Forecast Center in Colorado Springs, Colorado on 23 May.

Radar jamming

As the solar flare event unfolded on 23 May, radars at all three **Ballistic Missile Early Warning System (BMEWS)** sites in the far Northern Hemisphere were disrupted. These radars, designed to detect incoming Soviet missiles, appeared to be jammed. Any attack on these stations – including jamming their radar capabilities – was considered an act of war.



Retired Colonel Arnold L. Snyder, a solar forecaster at NORAD's Solar Forecast Center, was on duty that day. The tropospheric weather forecaster told him the NORAD Command Post had asked about any solar activity that might be occurring.

"I specifically recall responding with excitement, 'Yes, half the sun

has blown away,' and then related the event details in a calmer, more quantitative way," Snyder said.

Along with the information from the Solar Forecast Center, NORAD learned the three BMEWS sites were in sunlight and could receive radio emissions coming from the sun. These facts suggested the radars were being "jammed" by the sun, not the Soviet Union, Snyder said. As solar radio emissions waned, the jamming also waned, further suggesting the sun was to blame, he said.

During most of the 1960s, the Air Force flew continuous alert aircraft laden with nuclear-weapons. But commanders, thinking the BMEWS radars were being jammed by the Russians and unaware of the solar storm underway, put additional forces in a "ready to launch" status, according to the study.

"This is a grave situation," Knipp said. "But here's where the story turns: things were going horribly wrong, and then something goes commendably right."

The Air Force did not launch additional aircraft, and the study authors believe information from the Solar Forecasting Center made it to commanders in time to stop the military action, including a potential deployment of nuclear weapons. Knipp, quoting public documents, noted that information about the solar storm was most likely relayed to the highest levels of government – possibly even President Johnson.

The geomagnetic storm, which began about forty hours after the solar flare and radio bursts, went on to disrupt U.S. radio communications in almost every conceivable way for almost a week, according to the new study. It was so strong that the Northern Lights, usually only seen in or near the Arctic Circle, were visible as far south as New Mexico.

Societal impact

According to Snyder and the study authors, it was the military's correct diagnosis of the solar storm that prevented the event from becoming a disaster. Ultimately, the storm led the military to recognize space weather as an operational concern and build a stronger space weather forecasting system, he said.

The public is likely unaware that natural disasters could potentially trick contemporary military forces into thinking they are under attack, said Morris Cohen, an electrical engineer and radio scientist at Georgia Institute of Technology in Atlanta who was not involved in the new study.

"I thought it was fascinating from a historical perspective," he said of the new study.

The May 1967 storm brought about change as a near miss rather than a full-blown catastrophe, according to Cohen.

"Oftentimes, the way things work is something catastrophic happens and then we say, 'We should do something so it doesn't happen again,'" he said. "But in this case there was just enough preparation done just in time to avert a disastrous result."

— Read more D. J. Knipp et al., "The May 1967 Great Storm and Radio Disruption Event: Extreme Space Weather and Extraordinary Responses," Space Weather (accepted manuscript, 9 August 2016).

Belarus's lax approach to nuclear safety raises fear of another Chernobyl

Source: http://www.homelandsecuritynewswire.com/dr20160809-belarus-s-lax-approach-to-nuclear-safety-raises-fear-of-another-chernobyl

Aug 09- **Thirty years after Chernobyl, the world's worst nuclear accident, a series of mishaps at a nuclear facility in Astravets, in Belarus, has raised concerns over nuclear safety, especially in neighboring Lithuania.** Vilnius, the country's capital, is located less than thirty-one miles from Astravets. RFE/RL reports that in July, a nuclear reactor shell had been dropped while being moved. Local resident Nikolai Ulasevich, who is a member of the opposition United Civic Party, posted on his Facebook page that the 330-ton shell had fallen from a height of 2-4 meter in preparation for installation.

Two weeks later the Belarusian Energy Ministry confirmed that an "emergency

situation" had occurred at the construction site. It said that the incident took place at the warehouse facility, as the reactor was being moved.

Rosatom, the Russian state-owned company

which is the nuclear plant's main contractor, denied the reactor shell had been damaged in the fall, and said it will be installed as planned after supervisors give their permission.

These assurances notwithstanding, the Belarusian deputy energy minister Mikhail Mikhadyuk has said that the installation of the reactor shell was suspended until additional safety checks could be performed.

Lithuania did not hide its irritation with Belarus. The country's foreign minister, Linas Linkevicius, said the Soviet era-like lack of transparency by Belarusian officials was unacceptable. "These incidents, happening from time to time, lack of transparency, we're learning about them from open sources, usually too late…. This is not how it should be in reality. This last incident when a nuclear reactor vessel was possibly damaged is very dangerous," he said.

RFE/RL notes that Belarus is investing in nuclear power in an effort to lessen Belarus's dependence on Russian-supplied energy. Currently, about 90 percent of Belarus's gas imports come from Russia.

Analysts note, though, that the plant at Astravets is being built by Russian companies and Moscow is jointly financing the project, at an estimated cost of between $5 billion and $22 billion. Unit 1 of the construction is due to come online in 2018 and Unit 2 in 2020. Two other reactors are scheduled to be completed by 2025.

Soviet deja vu

The silence by President Alexander Lukashenko has angered many in Belarus as well.

Yury Varonezhtsau, a physicist and former parliamentary deputy, told RFE/RL: "For me it's a natural deja vu, as if I travelled back in a time machine a quarter of a century when we were investigating the causes of the Chernobyl disaster. Then, it was the same, but the difference was it was a totalitarian state, the Soviet Union, and now it's the supposedly democratic government of Belarus."

Other critics say Belarus has not properly performed an environmental-impact study for Astravets. One example: The power plant will draw water for its cooling reactors from – and release the warmed water back into — the Nevis River, which is one of the main sources of drinking water in Lithuania.

There were other accidents at the construction site, and all the

previous accidents were accompanied by ba refusal of the Belarus government to divulge any details.

In April, the structural frame of the nuclear service building at the site collapsed. According to the report by the Belsat independent TV station, site supervisors, under pressure to meet a fast-approaching deadline, ordered workers to pour too much concrete, causing the structure to collapse as a result of the additional weight.

The Belrus refused to comment on the accident, and a spokesman at the plant denyed anything had happened, even when shown videos of the collapsed structure. In May, the Belarusian energy ministry admitted an "incident" had occurred at the site, but that the "defect" had been dealt with.

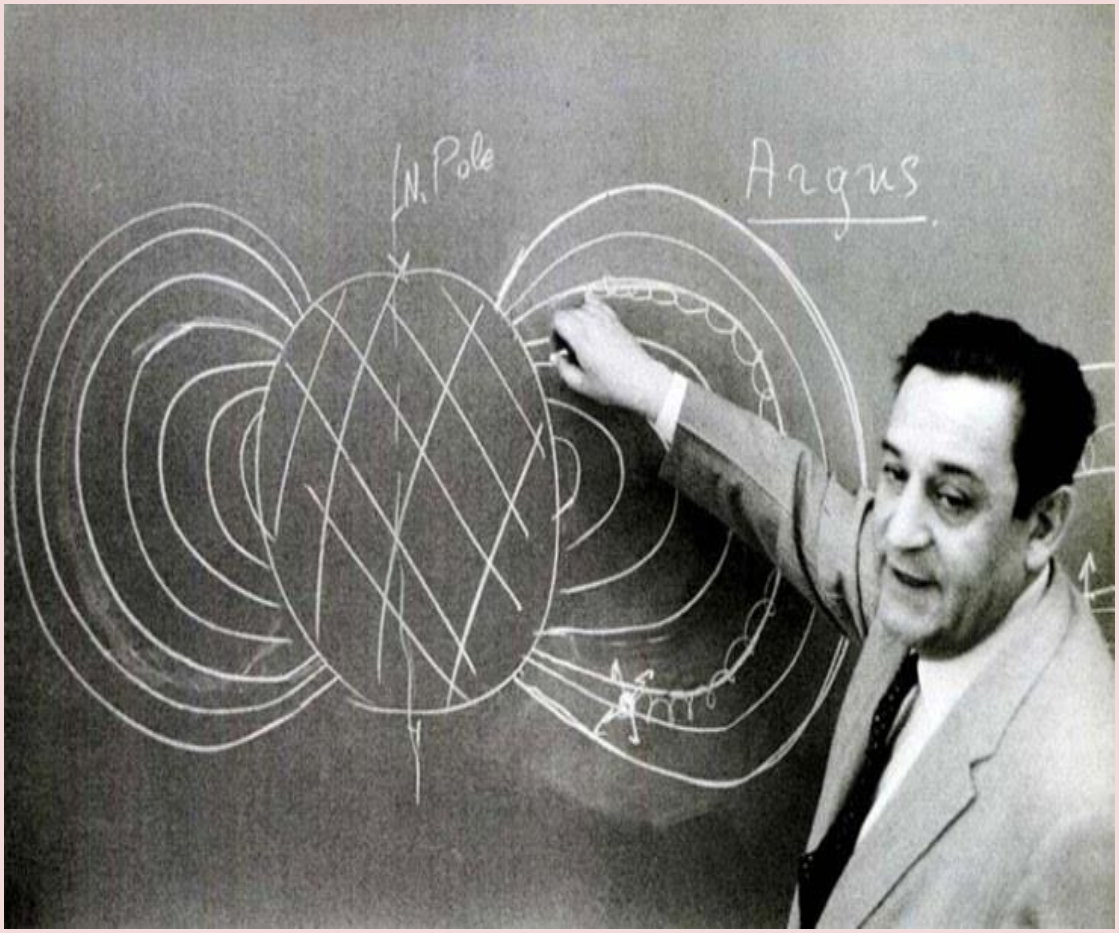
"All in all, we are really not satisfied with the process so far, and also we believe this is not just a bilateral problem, it's a regional [problem] and we would like to internationalize it as much as possible," Linkevicius said. **He noted that Lithuania agreed to close its own Ignalina nuclear facility as part of its 2004 accession agreement with the EU.**

Lithuanian president Dalia Grybauskaite said in late July that Vilnius would work with the international community to block the Astravets plant coming online if Belarus failed to adhere to international safety standards at the site.

The International Atomic Energy Agency (IAEA) director-general Yukiya Amano has said that the nuclear agency "has worked closely with Belarus on all aspects of this major project and will continue to offer every assistance." He said with two reactors under construction, Belarus "is one of the most advanced of what the IAEA calls 'newcomer' countries."

The "Crazy Greek"

Read more at: http://www.mlahanas.de/Greeks/new/Christofilos.htm



Nicholas Constantine Christofilos (Greek: Νικόλαος Χριστοφίλου; December 16, 1916 – September 24, 1972) was a Greek physicist. **Life Magazine, 30 March 1959:** "Triumph in Space for a Crazy Greek".

U.S. nuclear weapons in Turkey at risk of seizure by terrorists, hostile forces

Source: http://www.homelandsecuritynewswire.com/dr20160817-u-s-nuclear-weapons-in-turkey-at-risk-of-seizure-by-terrorists-hostile-forces

Aug 17 – The continued presence of dozens of U.S. nuclear weapons at Incirlik Air Base in Turkey raises serious risks of their seizure by terrorists and other hostile forces, a new report by the nonpartisan Stimson Center finds. The report, titled B61 Life Extension Program: Costs and Policy Considerations, found that it was an "unanswerable question" whether the United States could have maintained control of the approximately fifty B61 nuclear weapons based at Incirlik during a protracted civil conflict in Turkey. During the failed 15 July coup attempt, power to Incirlik Air Base was cut off and the Turkish government prohibited U.S. aircraft from flying in or out. Eventually, the Incirlik base commander was arrested and implicated in the coup plot. The Stimson Center notes that the report's findings come one month after the failed coup attempt and on the heels of a milestone earlier this month authorizing the production and engineering phase of the B61 Life Extension Program.

"From a security point of view, it's a roll of the dice to continue to have approximately fifty of America's nuclear weapons stationed at Incirlik Air Base in Turkey, just seventy miles from the Syrian border," said report co-author Laicie Heeley, a fellow with the Budgeting for Foreign Affairs and Defense program at the Stimson Center. "These weapons have zero utility on the European battlefield and today are more of a liability than asset to our NATO allies."

Over the next thirty years, the United States will spend an estimated $1 trillion to modernize the nuclear triad — which includes the B61 Service Life Extension Program. The National Nuclear Security Administration plans to extend the service lives of an

estimated 480 of the approximately 800 total B61 bombs at a projected total cost of more than $8 billion. The United States first deployed tactical nuclear bombs in Europe during the cold war in the late 1950s and early 1960s, to offset a buildup of Soviet tank armies deployed in Eastern Europe. Although most U.S. tactical weapons were withdrawn from Europe during the early 1990s, 180 of the tactical versions of the B61s remain at six bases in Europe — in Belgium, Italy, Germany, the Netherlands, and Turkey.

The report recommends the immediate removal of all B61 nuclear weapons from Europe and cancelling the procurement of B61s that would be stored in Europe. Doing so, the report finds, would create savings of more than $6 billion over the lifetime of the program, and free up additional military assets that could be used to bolster U.S. conventional forces.

"These bombs are ill-suited for modern warfare and incredibly costly," said report co-author Barry Blechman, co-founder of the Stimson Center. "The smart move would be to remove these weapons from Europe and double down to strengthen conventional forces that actually protect our NATO allies."

Hans Kristensen, the director of the Nuclear Information Project at the Federation of American Scientists, agrees with the conclusions of the Stimson Center's report. He told DW that political instability and the overall security situation in Turkey were reasons enough for the United States to pull its nuclear weapons out.

"There is no other country in Europe where the United States stores nuclear weapons where a military coup just happened and you have something that looks almost like a civil war with violent explosions and killings, and in addition to that you are less than 100 miles from the border of a completely war-torn country, Syria," he said.

"Those are security and political conditions that are completely out of sync with what you normally require for having nuclear weapons deployed," he added.

Over the years, security measures have been added to make the B61 bombs at Incirlik safer, but Heeley says this is beside the point. "There are a lot of safeguards in place…but when you are talking about U.S. nuclear weapons, if there is still a risk, you have to consider whether it is really worth taking that risk," Heeley told DW. "When we are talking about these particular weapons, the military value is not great enough to justify the risk you are taking."

Kristensen and Heeley reject the argument that the presence of the B61 bomb reassures Turkey about NATO's commitment to the country's defense, and that the withdrawal of these weapons would be taken as a signal of a weakening of that commitment.

"The B61s don't serve a military role in Europe… [withdrawing them] wouldn't hurt NATO security and may even help NATO security by focusing on conventional forces," Kristensen told DW.

Heeley agreed. "The United States in the past couple of years has invested significantly in [NATO]; they have put a lot of new conventional resources into the alliance," she said. "The United States should be able to show its support to Turkey in other ways through conventional support."

US moves nuclear weapons from Turkey to Romania

Source: https://www.euractiv.com/section/global-europe/news/us-moves-nuclear-weapons-from-turkey-to-romania/

Aug 18 – Two independent sources told EurActiv.com that the US has started transferring nuclear weapons stationed in Turkey to Romania, against the background of worsening relations between Washington and Ankara .

According to one of the sources, the transfer has been very challenging in technical and political terms.

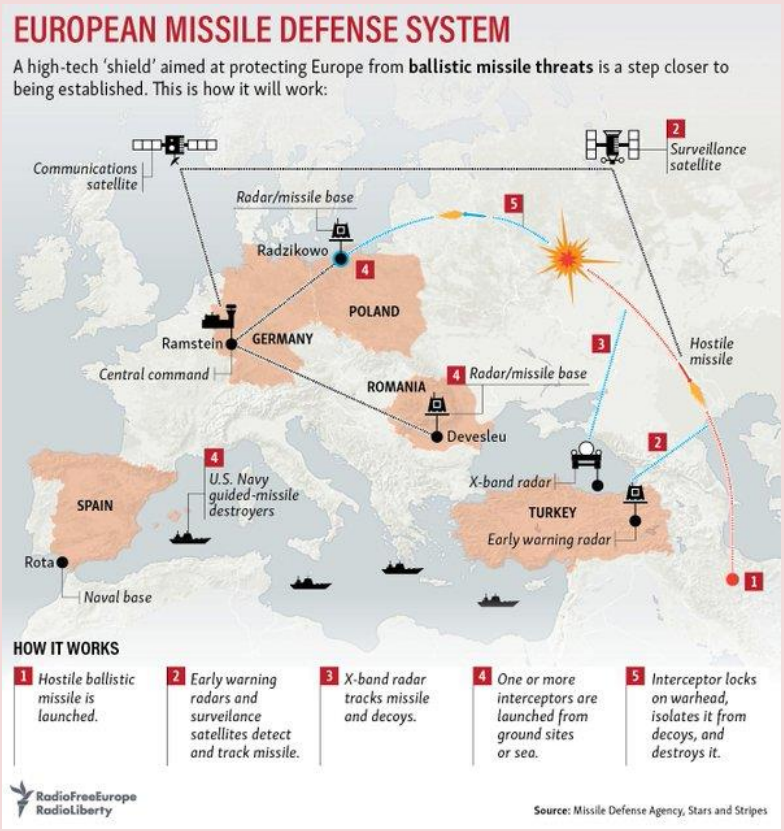
"It's not easy to move 20+ nukes," said the source, on conditions of anonymity.

According to a recent report by the Simson Center, since the Cold War, some 50 US tactical nuclear weapons have been stationed at Turkey's Incirlik air base, approximately 100 kilometres from the Syrian border.

During the failed coup in Turkey in July, Incirlik's power was cut, and the Turkish government prohibited US aircraft from flying in or out. Eventually, the base commander

was arrested and implicated in the coup. Whether the US could have maintained control of the weapons in the event of a protracted civil conflict in Turkey is an unanswerable question, the report says.

Another source told EurActiv.com that the US-Turkey relations had deteriorated so much following the coup that Washington no longer trusted Ankara to host the weapons. The American weapons are being moved to the Deveselu air base in Romania, the source said.



Deveselu, near the city of Caracal, is the new home of the US missile shield, which has infuriated Russia.

Romania was an ally of the Soviet Union during the Cold War, but it never hosted nuclear weapons during that period. Stationing tactical US nuclear weapons close to Russia's borders is likely to infuriate Russia and lead to an escalation. The stationing of Russian nuclear missiles in Cuba in 1962 was the closest the Cold War came to escalating into a full-scale nuclear war.

EurActiv has asked the US State Department, and the Turkish and the Romanian foreign ministries, to comment. American and Turkish officials both promised to answer. After several hours, the State Department said the issue should be referred to the Department of Defense. EurActiv will publish the DoD reaction as soon as it is received.

In the meantime, NATO sent EurActiv a diplomatically worded comment which implies that allies must make sure that US nuclear weapons deployed in Europe remain "safe".

"On your question, please check the Communiqué of the NATO Warsaw Summit (published on 9 July 2016), paragraph 53: "NATO's nuclear deterrence posture also relies, in part, on United States' nuclear weapons forward-deployed in Europe and on capabilities and infrastructure provided by Allies concerned. These Allies will ensure that all components of NATO's nuclear deterrent remain safe, secure, and effective," a NATO spokesperson wrote to EurActiv.

The NATO summit took place a few days before the failed coup in Turkey. At that time, the risks for the US nukes in Incirlik were related to the proximity of the war in Syria and the multiple terrorist attacks that have taken place in Turkey in recent months. For some of the attacks, Ankara blamed Islamic State, and for others the PKK, the Kurdish military organisation that appears on the EU and US terrorist lists.

Strong denial by Romania

The Romanian foreign ministry strongly denied the information that the country has become home of US nukes. "In response to your request, Romanian MFA firmly dismisses the information you referred to," a spokesperson wrote.

According to practice dating from the Cold War, leaked information regarding the presence of US nuclear weapons on European soil has never been officially confirmed. **It is, however, public knowledge that Belgium, the Netherlands, Germany and Italy host US nuclear weapons.**

After the failed putsch, relations between Washington and Ankara are at their worst since Turkey joined NATO in 1952. Ankara believes the US government supports the Turkish

US-exiled cleric Fethullah Gülen, whom it accuses of having masterminded the failed coup. Turkey is demanding Gülen's extradition, and the issue is expected to take center stage when US Vice President Joe Biden visits Turkey on 24 August.
Arthur H. Hughes, a retired US ambassador, wrote in EurActiv yesterday (17 August) that Gülen has indeed received considerable assistance from the CIA.

EDITOR'S COMMENT: Transfer has been verified – mainly because Turkish President demanded to have access to the US nuclear weapons at Incirlik AFB…

Long-term health effects of atomic bombs dropped on Japan not as dire as perceived

Source: http://www.homelandsecuritynewswire.com/dr20160816-longterm-health-effects-of-atomic-bombs-dropped-on-japan-not-as-dire-as-perceived

Aug 16 – The detonation of atomic bombs over the Japanese cities of Hiroshima and Nagasaki in August 1945 resulted in horrific casualties and devastation. **The long-term effects of radiation exposure also increased cancer rates in the survivors. But public perception of the rates of cancer and birth defects among survivors and their children is in fact greatly exaggerated when compared to the reality revealed by comprehensive follow-up studies.** The reasons for this mismatch and its implications are discussed in a Perspectives review of the Hiroshima/Nagasaki survivor studies published in the August issue of the journal *Genetics*, a publication of the Genetics Society of America.
"Most people, including many scientists, are under the impression that the survivors faced debilitating health effects and very high rates of cancer, and that their children had high rates of genetic disease," says Bertrand Jordan, an author and a molecular biologist at UMR 7268 ADÉS, Aix-Marseille Université/EFS/CNRS, in France. **"There's an enormous gap between that belief and what has actually been found by researchers."**

Dr. Jordan's article contains no new data, but summarizes over sixty years of medical research on the Hiroshima/Nagasaki survivors and their children and discusses reasons for the persistent misconceptions. GSA notes that the studies have clearly demonstrated that radiation exposure increases cancer risk, but also show that the average lifespan of survivors was reduced by only a few months compared to those not exposed to radiation. No health effects of any sort have so far been detected in children of the survivors.

Approximately 200,000 people died in the bombings and their immediate aftermath, mainly from the explosive blast, the firestorm it sparked, and from acute radiation poisoning. Around half of

the those who survived subsequently took part in studies tracking their health over their entire lifespan. These studies began in 1947 and are now conducted by a dedicated agency, the Radiation Effects Research Foundation (RERF), with funding from the Japanese and U.S. governments. The project has followed approximately 100,000 survivors, 77,000 of their children, plus 20,000 people who were not exposed to radiation.

GSA says that this massive data set has been uniquely useful for quantifying the risks of radiation because the bombs served as a single, well-defined exposure source, and because the relative exposure of each individual can be reliably estimated using the person's distance from the detonation site. The data has been particularly invaluable in setting acceptable radiation exposure limits for nuclear industry workers and the general public.

Cancer rates among survivors was higher compared to rates in those who had been out of town at the time. The relative risk increased according to how close the person was to the detonation site, their age (younger people faced a greater lifetime risk), and their sex (greater risk for women than men). However, most survivors did not develop cancer. **Incidence of solid cancers between 1958 and 1998 among the survivors were 10 percent higher, which corresponds to approximately 848 additional cases among 44,635 survivors in this part of the study. However, most of the survivors received a relatively modest dose of radiation. In contrast, those exposed to a higher radiation dose of 1 Gray (approximately 1000 times higher than current safety limits for the general public) bore a 44 percent greater risk of cancer over the same time span (1958-1998). Taking into consideration all causes of death, this relatively high dose reduced average lifespan by approximately 1.3 years.**

Although no differences in health or mutations rates have yet been detected among children of survivors, Jordan suggests that subtle effects might one day become evident, perhaps through more detailed sequencing analysis of their genomes. But it is now clear

that even if the children of survivors do in fact face additional health risks, those risks must be very small.

Jordan attributes the difference between the results of these studies and public perception of the long-term effects of the bombs to a variety of possible factors, including historical context.

"People are always more afraid of new dangers than familiar ones," says Jordan. "For example, people tend to disregard the dangers of coal, both to people who mine it, and to the public exposed to atmospheric pollution. Radiation is also much easier to detect than many chemical hazards. With a hand-held geiger counter, you can sensitively detect tiny amounts of radiation that pose no health risk at all."

Jordan cautions that the results should not be used to foster complacency about the effects of nuclear accidents or the threat of nuclear war. "I used to support nuclear power until Fukushima happened," he says. "Fukushima showed disasters can occur even in a country like Japan that has strict regulations. However, I think it's important that the debate be rational, and I would prefer that people look at the scientific data, rather than gross exaggerations of the danger."

— Read more in B. R. Jordan, "The Hiroshima/Nagasaki Survivor Studies: Discrepancies Between Results and General Perception," Genetics 203, no. 4 (August 2016): 1505-12.

UAE bolsters nuclear energy safety

Source: http://gulfnews.com/news/uae/government/uae-bolsters-nuclear-energy-safety-1.1882831

Aug 21 – **Nuclear energy experts from the United States are helping the UAE bolster existing border protection measures against illicit shipments of nuclear equipment or materials related to weapons of mass destruction,** said federal officials on Sunday.

The United States Department of Energy's International and Export Control programme experts met over three days with more than a dozen staff members of the UAE's Federal Authority for Nuclear Regulation (FANR).

The American export control programme is designed to "strengthen global efforts to prevent any unlicensed transfer of materials, equipment, and technology related to weapons of mass destruction (WMD), including nuclear weapons", said the UAE regulator.

Christer Viktorsson, director-general of FANR, told *Gulf News* on Sunday that training staff who review material transfers will enforce strict international agreements that call for only peaceful nuclear equipment and materials to be transferred across borders.

"As a party to the Nuclear Non-Proliferation Treaty, the UAE is committed to conducting only peaceful nuclear activities within its borders and also to working with the international community to prevent the illicit transfer of nuclear-weapon-usable materials and technologies," Viktorsson said in an interview on Sunday.

"Our recent workshop with the US Department of Energy assisted FANR staff members who review all trade applications to transfer nuclear-related items to, from, or through the UAE."

Viktorsson noted that effective "trade controls are essential tools in international efforts to prevent the proliferation of nuclear weapons, FANR is fully committed to its leading role in the UAE to support these non-proliferation strategies".

The workshop is part and parcel of new safety regulations imposed by FANR on the Western Region's

Barakah nuclear power plant where the first of four reactor units are expected to go online next year.

All four nuclear reactors are set for completion by 2020 to provide up to a quarter of the country's electricity demands yearly.

Federal powers of FANR staff as laid out under FANR's Regulation 9 were reviewed as part of the training for a better understanding of "national export control licensing, industry compliance, and inspections-based enforcement practices designed to prevent the uncontrolled transfer of sensitive items that could be used to build WMD", said the federal authority.

The UAE has pledged to use nuclear energy, equipment and technology "exclusively for peaceful purposes only and to implement import and export control rules for nuclear and nuclear-related equipment and technology in strict accordance with Nuclear Supplier Group (NSG) Guidelines for Nuclear Transfers. The NSG is a group of nuclear supplier countries that seeks to contribute to the non-proliferation of nuclear weapons through the implementation of two sets of guidelines for nuclear exports and nuclear-related exports", the authority said.

Ensuring inspections

According to FANR's Regulation 9 governing import and export of nuclear-related materials, UAE inspectors have full powers to inspect any shipment or premises involved in items related to nuclear power in the country.

The law reads that licensees "shall allow access, without any delay, to the authority to conduct an inspection, which the authority deems to be related to the transfer of regulated items, to verify the correctness and the completeness of the information provided and in compliance with the requirements of the law, this regulation and with conditions of the relevant licences".

The law also makes its clear that "the authority's inspectors are authorised to inspect industrial sites, stores or any other sites or locations in the state where regulated items are declared to be located, including, but not limited to, special and free zones in order to … ensure that such items are used for peaceful purposes in accordance with the obligations of the Treaty on the Non-Proliferation of Nuclear Weapons".

The regulations will help inspectors "investigate any suspicion that the transfer or end use of regulated items is unlicensed or unauthorised".

Reactor safety experts from Sandia help industry learn from Fukushima accident

Source: http://www.homelandsecuritynewswire.com/dr20160818-reactor-safety-experts-from-sandia-help-industry-learn-from-fukushima-accident

Aug 18 – **When you are an operator or engineer at a nuclear power plant, there are things you want to know long before you are faced with an emergency.**

Reactor safety experts from Sandia National Laboratories and elsewhere are sharing lessons learned in Japan's Fukushima Daiichi nuclear accident and other severe accidents that pushed nuclear power plants past their limits. They are passing on what they know to operators and engineers through the Technical Support Guidelines (TSG) Skillset Workshops, developed by the General Electric Boiling Water Reactor (BWR) Owners' Group.

Sandia Lab says that the workshops seek to demystify what happens during an accident, to help engineers/operators learn what decisions they might need to make in the event of an accident at their plants, and to provide insights into the non-intuitive nature of accidents. To date, workshops have been held in Taiwan, Japan, and at Sandia and elsewhere in the United States, with more workshops planned for Switzerland, Mexico, Spain, and the United States.

What to expect next

"By walking participants step-by-step through what happened during a real-world accident, operators/engineers can use that information to know where they are in the accident process, so they know what to expect next, particularly when the accident could progress in ways that are unexpected," said Randy Gauntt,

manager of Sandia's Severe Accident Analysis Department.

Sandia brings decades of experience to the workshops. Its analytical software, developed for the Nuclear Regulatory Commission (NRC), was used to advise the NRC, Department of Energy, and TEPCO, the Tokyo Electric Power Company, as the accident progressed at Fukushima Daiichi.

Sandia began studying responses to severe nuclear accidents shortly after the Three Mile Island incident in Pennsylvania in 1979, an event that radically altered the future of nuclear power in the U.S. Since then, Sandia has provided research and support for investigations into severe reactor accidents to industry worldwide and to U.S. and foreign regulatory agencies, and serves as the NRC's principal contractor for severe accident research.

Accidents progress in surprising ways

Not all plant accidents are the same. Some things about Fukushima were surprising. **"Pumps that should have failed in a few hours ran for days, well beyond their expected design basis,"** said Douglas Osborn, a technical staff member at Sandia.

Osborn said that in the Fukushima accident, the expected reactions that create hydrogen led to explosions in the Units 1, 3, and 4 reactor buildings.

"As the core heated to temperatures of more than 1,800 F (about 1,000 C), the fuel cladding metal reacted with the steam in an exothermic oxidation reaction, leading to rapid temperature increase to the point where water didn't provide sufficient cooling and created large amounts of hydrogen. The cladding and fuel began to melt, while cladding oxidation continued," Osborn said.

He said the **reactor core material failed at the bottom of the reactor vessel**, and the molten core material freed water, hydrogen, carbon monoxide and carbon dioxide from the concrete as well. When the core material mixed with zirconium and steel oxidized on the concrete, large quantities of combustible gas, hydrogen and carbon monoxide is generated, creating additional heat. The combustible gases may have burned above the molten pool or may have accumulated with the other gases to pressurize the containment vessel, Osborn said.

Many of these accident progressions are still being analyzed with the data from the Fukushima accident to determine the conditions of the core and provide insights that will help engineers and operators prevent another accident.

Training the next generation

The TSG Skillset Workshops help operators/engineers understand severe accident phenomena and timelines so they can recognize critical events, and helps them identify limitations of tools and equipment, including those needed to assess and predict the accident's progression.

"The next generation of nuclear professionals understands better the events that have impacted the industry through lessons this generation has learned," said Bill Williamson, chair of the BWR Owners' Group Emergency Procedures Committee.

Sandia Lab notes that Williamson and others in the group are working to ensure that workshops like the one at Sandia transfer vital information that allows nuclear professionals to better interpret severe accident instrument readings. Williamson said severe accident conditions do not lend themselves to simple, easy-to-understand instrument readings, increasing the importance of the workshops.

"Ultimately, we want the operators to know that they aren't alone if an accident occurs at their plant. We want them to know that there are tools to help them, and there are experts who they can turn to," Osborn said.

Explosion Detecting Sensors Possibly Deployed in US Public Places

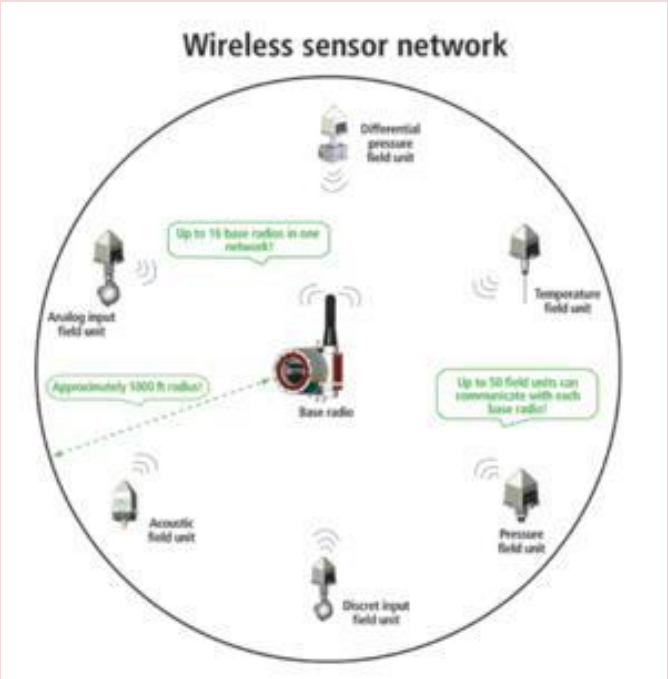
Source: http://i-hls.com/2016/07/explosion-detecting-sensors-possibly-deployed-in-us-public-places/

July 22 – **A conflict between the principles of civil rights and security requirements has been reflected by the attempt of US defense authorities to install explosion detecting sensors in public places.**

A US Defense Department agency wants to install explosion-detection equipment on public property somewhere in Arlington, Virginia., and is asking the County Board to **keep details about the equipment and its location secret.**

According to Stars and Stripes, the proposal is being opposed by the American Civil Liberties Union of Virginia.

Arlington is home to the Pentagon, one of the sites attacked on Sept. 11, 2001. Reagan National Airport and multiple other federal facilities are also located there.



The system is designed to "characterize" explosions in urban environments, according to the Defense Threat Reduction Agency (DTRA). It would collect information that could help law enforcement prosecute suspects and assess damage.

"In the event of an intentional detonation such as a terrorist attack, information generated by the system is critical for the Federal government's efforts to determine who was responsible for and how to respond to the event," wrote Air Force Col. D. Brent Morris.

"However, **disclosure of the location** of our equipment and information regarding its components and operation would jeopardize the ability for the system to provide valuable information in a timely fashion . . . by giving insight into the system's design and coverage and possibly how to defeat the system."

The defense agency said the network of sensors it wants to install would monitor "seismic, sound, air pressure, radiation, light, and radio frequency signals to help determine the size, location, and other characteristics of an explosion. All of the sensors being installed are passive until triggered by an event, and do not at any time record video or voice data."

The agency's statement said such sensors have already been installed in other U.S. cities, though it did not say which ones.

Science Magazine disclosed in March that there has been a government-wide effort to upgrade old blast sensors systems from a number of cities and link them into a network that would be operable as of 2018 and has been named **"Discreet Oculus"** which can be deployed in and around cities. A portable version is also planned.

Arlington County Manager has recommended approval of the request to install the sensors and keep the details secret. The defense agency's request for secrecy cites a section of the Virginia Freedom of Information Act that allows the government to withhold information if doing so would prevent terrorist activities or cyberattacks or aid the response to such attacks.

But the ACLU of Virginia said that without more information, "citizens can have no assurance that the equipment … does not have the capability of recording private conversations conducted in public spaces or of invading personal privacy in other ways."

The ACLU is not asking for the location of the sensors, she said, but is still concerned about the technology.

Ansbach explosion: Syrian asylum seeker killed by own bomb at German bar

Source: http://www.telegraph.co.uk/news/2016/07/24/one-dead-and-ten-injured-after-restaurant-blast-in-german-city-o/

July 25 – A suicide bomber who blew himself up after being turned away from a music festival in southern Germany was a Syrian man who had been denied asylum, according to Bavarian authorities.
The 27-year-old killed himself and injured 12 others when he detonated an explosive device after being denied entry to the event in Ansbach because he didn't have a ticket, the Bavarian interior minister said.

Around 2,500 people attended the open-air festival, local news reported.
"We don't know if this man planned on suicide or if he had the intention of killing others," Joachim Herrmann said, adding that three of the 12 victims suffered serious injuries.
"Unfortunately, this is a terrible new attack which will surely increase people's anxiety," Mr Herrmann said.
He said that the contents of a backpack that the man was carrying would have been sufficient to kill and injure many more people.

Mr Herrmann said that the attacker, who came to Germany two years ago but had his asylum claim rejected after a year, had tried to kill himself twice in the past and had spent time in a psychiatric clinic.

He added that he was worried "the right to asylum would be undermined" by the events of the past week, which has seen attacks on a train and shopping mall in the southern German state.

A spokesman for the prosecutor's office in Ansbach said the attacker's motive wasn't clear.
"If there is an Islamist link or not is purely speculation at this point," said the spokesman, Michael Schrotberger.
Deputy police chief Roman Fertinger said there were "indications" that pieces of metal had been added to the explosive device.
On Sunday night police said they suspected that the man who had died in the explosion was the attacker.
"An explosion went off in the city centre and a man, who the latest enquiries show caused it, was killed in the event," Ansbach police said in a statement.
The area around Eugene's Wine Bar was sealed off by police after the explosion, which was first reported shortly after 10pm local time.

Witnesses of the incident described seeing a rucksack explode, killing the man.
Ansbach deputy police chief Roman Fertinger said there were "indications" pieces of metal had been added to the explosive device.
The perpetrator was killed in the explosion,

police said in a statement, and a spokeswoman said 12 people were wounded, three of them seriously.
Emergency services including police and rescue workers were called to the central square of the city. A helicopter was also at the scene.
Bavarian public broadcaster Bayerische Rundfunk reported that about 200 police officers and 350 rescue personnel were brought in following the explosion in Ansbach.
Initial reports had suggested that the blast was the result of a gas explosion, but Carda Seidel, the mayor of Ansbach, said it had been caused by an explosive device, local news website Nordbayern.de reported.
“The explosion was set off deliberately,” said Michael Siefener, a spokesman for the regional interior ministry, adding that authorities were trying to establish the exact cause.
The website of the German newspaper, Bild, reported that it could not be ruled out that there were multiple explosions.
She was quoted by Munich’s Focus magazine as saying that the explosion was near the entrance to an open-air music festival. The three-day concert, with about 2,500 attending, was said to have been shut down as a precaution after the explosion.
The city of Ansbach is in Bavaria, some 124 miles (200km) north of Munich.
Ansbach is home to a US Army base and the 12th Combat Aviation Brigade. A spokesman at the base said the base had no information about the explosion.
Germany has been on high alert following the recent events in Munich.

The pack back used to carry an explosive device is seen at the scene of a suicide attack in the southern German city of Ansbach Credit: AFP/Getty

Two days earlier, an 18-year-old man killed nine people in a shooting outside a McDonald’s near a shopping centre in Munich, before then killing himself nearby.
After the Munich attack, Mr Herrmann urged the German government to allow the country's military to be deployed to support police during attacks. Germany's post-war constitution only allows the military to be deployed domestically in cases of national emergency.
Mr Herrmann has called those regulations obsolete and said that Germans have a "right to safety."
Back in January, Bavaria's justice minister launched a state program in Ansbach meant to teach refugees the basics of law in their new host country, amid growing tensions and concerns in Germany about how it would integrate the estimated one million-plus migrants it registered crossing into the country last year. Classes include lessons about freedom of opinion, the separation of religion and state and the equality of men and women.
"Germany is an attractive country because it respects the dignity of every human being," an educational film shown to newcomers said, "and it is supposed to stay that way."

Syria car bomb: Isis claims responsibility after attack in northern city of Qamishli kills at least 44 people

Source: http://www.independent.co.uk/news/world/middle-east/syria-car-bomb-bombing-truck-attack-al-qamishli-map-today-death-toll-latest-news-a7157616.html

July 27 – Isis has claimed responsibility after least 44 people were killed and more than 100 wounded in a **twin bombing** in a predominantly Kurdish town in the north of Syria.
Syrian state-TV said a truck loaded with explosives blew up on the western edge of the town of **Qamishli, near the Turkish border.**

Minutes later the attack was followed by a blast from an explosives-packed motorcycle in the same area.

The blasts caused massive damage to the area and rescue teams are working to recover victims from under the rubble.
The town is mainly controlled by Kurds but Syrian government forces are present and control the airport.
Isis claimed responsibility for the attack through its propaganda agency Amaq, which said over 100 had been killed in a truck bombing attack on the headquarters of "Kurdish units".
The bomber drove a cattle van and used live sheep for camouflage, the Hawar news agency reported.

US Follows Islamic Terrorists' Use of Explosive UAVs

Source: http://i-hls.com/2016/07/us-follows-islamic-terrorists-use-of-explosive-uavs/

July 28 – Warfare against IEDs (improvised explosive devices) has been on the US Defense Administration agenda for a long time. Lessons have been learned also from Israel's operational activities in this field. In mid-2016 the U.S. Department of Defense asked Congress for an additional $20 million to develop countermeasures to the growing Islamic terrorist use of cheap commercial UAVs. The Islamic terrorists, especially ISIL (Islamic State in Iraq and the Levant), have been using these UAVs more frequently in the last few years and the Department of Defense believes ISIL is planning to eventually use these commercial UAVs as flying bombs. The defense administration organization JIDO has long been working on better ways to detect and deal with non-flying IEDs and considers bomb equipped UAVs a flying IED.
The Department of Defense points out that since September 11, 2001 two-thirds of the Americans killed in combat were the victims of IEDs in the form of roadside bombs and (much less often) mines. JIDO, that has been spotting and defeating bomb equipped commercial UAVs, wants more money to get results faster.
There have been electronic chatter among Islamic terrorists about the possibility of armed commercial UAVs. According to Strategy Page, U.S. counter-IED tactics concentrate on discovering who is organizing the IED effort, and then going after the key members of that organization. This is done using a combination of powerful computer software, and traditional detective and military intelligence methods. Those same methods have been picking up more discussions about using commercial UAVs and eventually arming them.
JIDO found out that the most effective tactic was to take out the leaders and technical specialists (bomb builders). That worked in Iraq, it worked in Afghanistan and worked in Israel.
Going after commercial UAVs is not just to eliminate explosive UAVS but also unarmed UAVs used for reconnaissance by Islamic terrorists. For the moment the Islamic terrorists do not have enough UAVs for anything but reconnaissance. These are often shot down or lost due to equipment failure or operator error. Money is often scarce in Islamic terror groups and there are more urgent priorities (like more guns, bullets and food). But the Department of Defense believes it's only a matter of time and wants to be ready.

Suicide bomber kills at least 70 at Pakistan hospital

Source: http://www.reuters.com/article/us-pakistan-blast-idUSKCN10J0I7

Aug 08 – A suicide bomber in Pakistan killed at least 70 people and wounded more than a hundred on Monday in an attack on mourners gathered at a hospital in Quetta, according to officials in the southwestern province of Baluchistan.

The bomber struck as a crowd of mostly lawyers and journalists crammed into the emergency department to accompany the body of a prominent lawyer who had been shot and killed in the city earlier in the day, Faridullah, a reporter who was among the wounded, told Reuters.

Abdul Rehman Miankhel, a senior official at the government-run Civil Hospital, where the explosion occurred, told reporters that at least 70 people had been killed, with more than 112 wounded, as the casualty toll spiked from initial estimates.

"There are many wounded, so the death toll could rise," said Rehmat Saleh Baloch, the provincial health minister.

Jamaat-ur-Ahrar, a faction of the Islamist militant Pakistani Taliban group, claimed responsibility for the attack in an email.

It was not immediately clear if the group had carried out the bombing, as it is believed to have claimed responsibility for attacks in the past that it was not involved in.

"The Tehreek-e-Taliban Pakistan Jamaat-ur-Ahrar (TTP-JA) takes responsibility for this attack, and pledges to continue carrying out such attacks," said spokesman Ehsanullah Ehsan in the statement.

Only last week, Jamaat was added to the United States' list of global terrorists, triggering sanctions.

Television footage showed scenes of chaos at the hospital in Quetta,

with panicked people fleeing through debris as smoke filled the hospital corridors.

Bodies lay strewn across a hospital courtyard

shortly after the blast and pools of blood collected as emergency rescuers rushed to identify survivors.

Prime Minister visits

The motive behind the attack was unclear, but several lawyers have been targeted during a recent spate of killings in Quetta, the provincial capital of Baluchistan which has a history of militant and separatist violence.

The latest victim, Bilal Anwar Kasi, was shot and killed while on his way to the city's main court complex, senior police official Nadeem Shah told Reuters. He was the president of Baluchistan Bar Association.

The subsequent suicide attack appeared to target his mourners, Anwar ul Haq Kakar, a spokesman for the Baluchistan government, said.

"It seems it was a pre-planned attack," he said.

Ali Zafar, president of the Supreme Court Bar Association of Pakistan, told reporters in the eastern city of Lahore:

"We (lawyers) have been targeted because we always raise our voice for people's rights and for democracy...Lawyers will not just protest this attack but also prepare a long-term plan of action."

Police cordoned off the hospital following the blast, with Prime Minister Nawaz Sharif and Army Chief General Raheel Sharif paying visits to the wounded on Monday evening.

In January, a suicide bomber killed 15 people outside a polio eradication centre in an attack claimed by both the Pakistani Taliban and Jundullah, another Islamist militant group that has pledged allegiance to Islamic State in the Middle East.

Monday's attack was the worst in Pakistan since an Easter Day bombing ripped through a Lahore park, killing at least 72 people. Jamaat-ur-Ahrar also claimed responsibility for that atrocity.

Quetta has long been regarded as a base for the Afghan Taliban, whose leadership has regularly held meetings there in the past.

In May, Afghan Taliban leader Mullah Akhtar Mansour was killed by a U.S. drone strike while traveling to Quetta from the Pakistan-Iran border.

Dog owners warned about "tennis ball bombs" ahead of Fourth of July weekend

Source: http://www.cbsnews.com/news/dog-owners-warned-about-tennis-ball-bombs-ahead-of-fourth-of-july-weekend/

June 29 – It's unusual for dog owners to steer clear of tennis balls, but this Fourth of July, they're being told to do just that.

Ahead of the holiday weekend, police are issuing warnings about homemade fireworks -- "tennis ball bombs" in particular.

People take the insides of fireworks out, put the explosive material in objects such as pipes, ping pong balls or tennis balls, add a wick and then set them off -- with sometimes terrible consequences.

"Some of them are very effective and dangerous, and some of them don't work, but you don't know," Jarod Kasner, public information officer for the Kent Police Department in Washington state, told CBS News. "People light them, leave them thinking it's a dud, but who knows what's happening on the inside. Then a dog comes and picks it up..."

That's why police departments like Kent are warning residents to be cautious if they see an abandoned item.

In 2000, a Portland man was reportedly on a walk with his dog when he spotted a tennis ball in the grass. Without giving it a second thought, the man picked up the ball and tossed it to the pup.

When the dog bit down, the ball exploded, CBS Sacramento reports; the pet had to be euthanized immediately.

"If it doesn't go 'boom' some people just walk away from it," Kasner said. "Unfortunately, dogs pick up everything up in their mouth and bring it to you."

There's a serious hazard for people, too, Kasner explained, because there's a chance the explosive ball could go off in your hand.

"It could be smoldering on the inside and when you move it around that's when it goes off," Kasner said.

If you see a ball or any other household item that looks burnt or has a wick or tape attached to it, don't touch it, police warn.

Innovative Drone to Demine World Land Mines

Source: http://i-hls.com/2016/08/innovative-drone-to-demine-world-land-mines/

Aug 04 – **There are 100 million land mines in more than 60 countries worldwide. Every day, 10 innocent civilians are killed or maimed by these explosives**

The **Mine Kafon Drone** (MKD), a prototype of airborne demining system, has been raising money on Kickstarter, and Its developer says the drone will clear all land mines around the world in less than a decade.

According to the company's Kickstarter page and website, the Mine Kafon Drone is an unmanned

airborne demining system that uses a three-step process to map, detect and detonate land mines up to 20 times faster than currently available technologies.

The system delivers accurate updates and information on mine clearing operations.

Flying over dangerous areas to map, detect and detonate landmines from a safe distance. **The drone works autonomously, and is equipped with three separate interchangeable robotic extensions:**

Mapping – First the drone flies over the whole field with an aerial 3D mapping system to identify all the dangerous areas with GPS way points.

Detection – Equipped with a robotic metal detecting arm the MKD hovers above the ground at approximately 4 cm to detect mines. Every detected mine is geotagged on the operator's system to construct a map of known mine locations.

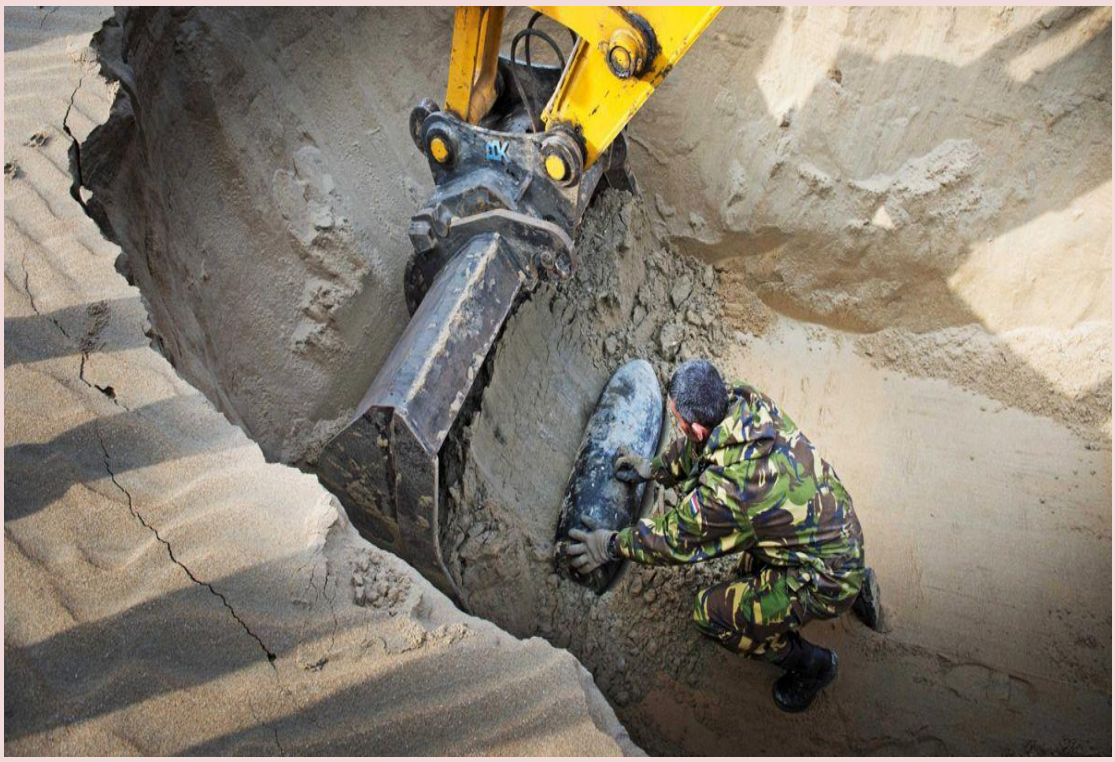
Destroying – Attached with a robotic gripping arm, the drone places a small detonator on every detected mine. The land mine is then detonated from a safe distance using a timer.
The innovator, Afghanistan-born Massoud Hassani, moved to the Netherlands as a teenager and went on to graduate from Eindhoven's celebrated Design Academy. He created the Mine Kafon, a wind powered spherical device that rolls across minefields, detonating landmines on contact, as his graduation projec. This award-winning invention has met with international acclaim. Later he devloped the drone at its present model.

Unexploded Bomb from WWII Found at VW's Headquarters

Source: http://www.motortrend.com/news/unexploded-bombs-wwii-found-vws-headquarters/

July 12 – Explosive experts defused a World War II-era bomb that was found at Volkswagen's headquarters in Wolfsburg, Germany.
Construction workers first found suspicious metal pieces at four different locations inside Volkswagen's headquarters last month. On Friday, experts began searching the large plant for an explosive device. Sure enough, they found a **250-kg (550-pound) bomb** at the VW factory, reports local news agency *Wolfsburger Allgemeine Zeitung*. Almost 700 people had to be evacuated from the Sandkamp district near the plant, and police, fire fighters, and aid organizations were on hand at the site just in case. Fortunately, the whole process went along safely without a hitch, according to the report.

Considering the Wolfsburg facility played a large role in Germany's war efforts, it's not surprising that allied bombs have cropped up at the plant over the years. In 1938, the Wolfsburg factory was built to create the People's Car on Adolf Hitler's orders. Later, the plant produced military vehicles and aircraft supplies for use in the war.



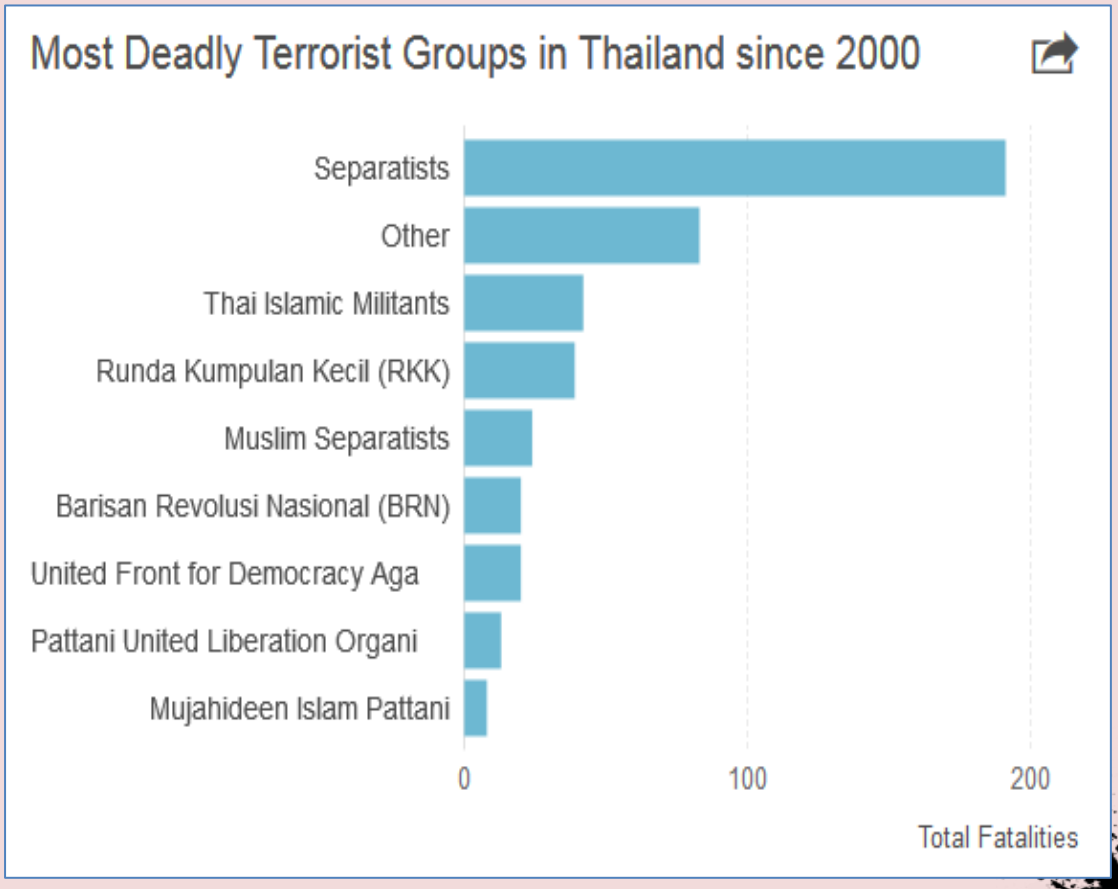
String of bomb blasts strike Thai resorts

Source: http://www.foxnews.com/world/2016/08/12/string-bomb-blasts-strike-thai-resorts.html

Aug 12 – Police in Thailand have confirmed that another person has died in a new bomb blast in the southern resort city of Hua Hin.

Police Lt. Gen. Samer Yousamran said Friday that three people were also wounded in the blast.

The explosion came hours after twin explosions killed one woman and wounded around 20 in Hua Hin late Thursday.



Trang	1 IED	1 dead, 6 wounded
Hua Hin	2 IEDs	1 dead, 26 wounded
Surat Thani	2 IEDs	1 dead, 4 wounded
Phuket, Patong beach	1 IED, 1 IED defused	1 wounded
Nakon SriThamarat	1 IED	??
Hua Hin	1 IED, 1 IED defused	4 injured
Phang Nga	2 IEDs	so far none reported.
In addition, fires/arson attacks in Phang Nga, Krabi, Trang and Surat Thani (these may be above mentioned IEDs. For the record, many bombs in the Deep South are "incendiary IEDs", ie, designed for arson, not explosions). 2 people dead.		

Several other blasts have also been reported in other cities in southern Thailand.

Explosion at hospital on Turkey's Syrian border leaves at least 50 people injured

Source: http://counteriedreport.co.uk/explosion-at-hospital-on-turkeys-syrian-border-leaves-at-least-50-people-injured

Aug 10 – The blast at Mardin State Hospital near the border with Syria was heard miles away and has left a huge plume of smoke trailing over the area

At least 50 people have been injured following an explosion at a hospital in Turkey.

The blast at Mardin State Hospital in Kızıltepe on the border with Syria was heard miles away and has left a huge plume of smoke trailing over the area.

Turkey has been rocked in recent months by terror bombings claimed by ISIS militants, as well as PKK Kurdish separatists.
It is currently unclear what has caused this most recent blast however.

How the IED changed the U.S. militar

Source: http://www.usatoday.com/story/news/nation/2013/12/18/ied-10-years-blast-wounds-amputations/3803017/

Combat engineers inspect a bridge

2013 – Three sets of eyes peer out of a massively armored U.S. truck rolling slowly down Highway 1.
From inside their reinforced cocoon — constructed layer upon layer with ways to protect the human cargo inside — three Arizona National Guard Army engineers scan highway edges. They look for signs of digging, suspicious debris or any other anomaly in the dirt that hints at a buried explosive.
The rate of Americans dying or becoming dismembered by improvised explosive devices (IEDs), for 10 years the tormentor

of U.S. forces, has dropped sharply as coalition troops withdraw from the battlefield. But lives still depend on what soldiers see or don't see. It's an enduring legacy of the homemade bomb that has created more American casualties over a decade and two wars than any other weapon.

What someone didn't see in the dirt along this same highway just 12 weeks earlier was a buried IED weighing hundreds of pounds. It killed 1st Lt. Jason Togi, 24, of Pago Pago, American Samoa, and an Afghan interpreter on a similar convoy mission riding in the same type of RG-31 armored truck.

"There's certain catastrophic explosions that it does not matter if you're in some sort of titanium ball," said Col. William Ostlund, commander of U.S. troops in this province.

So in the cramped quarters of the RG-31 this day, amid the smell of beef jerky and the cases

of Burn and Rip It energy drinks, there lurks in the recesses of every soldier's mind one thought. Spc. Kyle Esplin, 22, who waits tables in Tucson; Spc. Brody Crane, 24, a part-timer at a Bass Pro Shop in Mesa, Ariz.; and Sgt. 1st Class Ramon Gomez, 33, who has a 5-month-old son, Emilio, back in Tucson, know that everything in their world could end in a violent millisecond.

"You don't want to think about it," Crane says over the vehicle intercom system.

Somewhere between more than half to two-thirds of Americans killed or wounded in combat in the Iraq and Afghanistan wars have been victims of IEDs planted in the ground, in vehicles or buildings, or worn as suicide vests, or loaded into suicide vehicles, according to data from the Pentagon's Joint IED Defeat Organization or JIEDDO.

That's more than 3,100 dead and 33,000 wounded. **Among the worst of the casualties are nearly 1,800 U.S. troops who have lost limbs in Iraq and Afghanistan, the vast majority from blasts, according to Army data.**

A lethal weapon

When one of the first Americans serving in Iraq, 25-year-old Pfc. Jeremiah Smith, 25, of Odessa, Mo., died in an explosion under his vehicle in May 26, 2003, six weeks after the U.S. invasion ended, the military wasn't even sure what to call the thing that killed him.

The Defense Department inadvertently applied an oxymoron, saying he was "hit by unexploded ordnance." Officials couldn't possibly know at the time that this weapon — what would come to be called in military parlance an improvised explosive device, a term now in common usage by those in and

out of uniform — would be the most destructive of two wars.

The terror of the weapon continues to this day. Even as American forces leave Afghanistan, small numbers of U.S. soldiers gamble their lives on bomb-ridden roads or pathways.

November marked 10 years since the first U.S. death in Afghanistan blamed, when it happened, on an IED: Sgt. Jay Blessing, an Army Ranger, killed when the "thin-skinned" or unarmored Humvee he was driving was hit by a buried bomb Nov. 14, 2003.

The military has since gone back to identify a few earlier cases that technically qualify as IED attacks, including the death of Navy SEAL Matthew Bourgeois, 35, of Tallahassee, from a land mine wired to homemade bombs near Kandahar on March 28, 2002.

The IED, made for as little as a few hundred dollars each and produced by the thousands yearly first in Iraq and then Afghanistan, has changed the arc of how America wages war and how military medicine cares for the wounded.

It is a considerable feat for a triggering device made of wood and wire. Displayed at an IED investigative office at Bagram Air Base, they look like junior high workshop projects.

The bombs radically affected how the American military could move around the war zone, creating a heavy reliance on helicopters and other aircraft in order to avoid roads, says Army Lt. Gen. John Johnson, JIEDDO director.

"They've caused us a lot of pain ... a lot of effort and a lot of treasure," Johnson says.

Hundreds of millions in research dollars have been spent on understanding, identifying and treating the twin invisible maladies most often associated with these bombs: traumatic brain injury and post-traumatic stress disorder. Military and private researchers estimate the number of uniformed victims in the hundreds of thousands.

The IED has given rise to a multibillion-dollar industry in vehicle and body armor, robots, ground-penetrating radar, surveillance, electrical jamming, counterintelligence, computer analysis and computerized prostheses.

The Government Accountability Office says it's impossible to estimate the total U.S. cost of fighting the bombs over two wars. But the Pentagon has spent at least $75 billion on armored vehicles and tools for defeating the weapons.

In 2007, when American troops were losing limbs from blasts about every other day on average, the word IED — a military acronym for "improvised explosive device" — was so widely used it formally entered the American lexicon, accepted into Merriam-Webster's Collegiate Dictionary.

Fours year later, at the height of the Afghanistan War, the pace of U.S. troops suffering major amputations increased to one every 36 hours.

Surviving a blast

They call it "going boom." The first time for Spec. Leif Skoog, 23, a roofer back in Phoenix, was Oct. 3. He and Crane were in an RG-31 that was pushing an 8,000-pound roller in front of the vehicle, a device designed to detonate anything buried before the truck passes over it.

That's exactly what happened. The roller was destroyed, but the RG-31 survived. For those inside, there was the shock of the explosion, painful ear pressure, air made black with billowing dirt and dust, and a chemical smell that burned the nostrils.

Skoog, closer to the blast in the driver's seat, was stunned and disoriented. "It's not a physical wound," he recalls. "It's more like something doesn't feel right."

He showed signs of a mild traumatic brain injury from blast exposure, what scientists call the signature wound of the Iraq and Afghanistan wars. With dizziness, headaches and minor concentration problems, Skoog was kept out of combat for two weeks.

Understanding the frequency of these wounds in a war where body and vehicle armor block shrapnel but the IED blast wave can still damage the brain was one of the hardest lessons learned by military medicine from modern wars.

"It was like a slow awakening for everybody," says Chris Macedonia, a doctor and former adviser to the chairman of the Joint Chiefs of Staff, now-retired admiral Michael Mullen. "There were phenomena that were happening, particularly related to IEDs, that just didn't match what the education and teaching were before."

Doctors found that repeated mild brain injuries from blasts — without allowing the brain time to heal — can cause permanent neurological damage, risking later onset of Alzheimer's, Parkinson's or the even more

debilitating chronic traumatic encephalopathy.

A RAND Corp. report estimated in 2008 that perhaps 320,000 troops, even at that early date, had suffered concussions or mild brain injuries, mostly from blast exposure. Pentagon officials the next year put the number at 360,000.

Most were never diagnosed when the wounds occurred and sent right back into combat, and no one knows the accurate number today, says Terri Tanielian, a RAND senior research analyst.

Not until 2010, nine years into the fighting, did three military leaders — Mullen; retired general Peter Chiarelli, then-Army vice chief of staff; and Marine Commandant James Amos — push through sweeping battlefield treatment changes requiring blast-exposed troops to be pulled from combat until, as with Skoog, symptoms go away.

"It took us a long, long time," Macedonia says. "Too long."

More protection for troops

As early as 2003, U.S. field commanders in Iraq began demanding for their troops something other than the boxy Humvees that were being ripped apart by this new weapon.

Soldiers and Marines had taken it upon themselves to add so-called Hillbilly armor to their vehicles or pile sandbags on the floorboards.

The Pentagon initially rushed kits to retrofit Humvees with better protection in 2003 and 2004. But the trucks remained vulnerable because of their "flat bottom, low weight, low ground clearance and aluminum body," a Pentagon inspector general report found.

A Bush administration certain the Iraq War would be short-lived failed to supply large numbers of new Mine Resistant Ambush Protected (MRAP) trucks like the RG-31 until 2007. In the meantime, more than 1,400 U.S. troops died in IED blasts and 13,000 were wounded, according to JIEDDO data.

It was a USA TODAY story about the effectiveness of a limited number of MRAPs in saving the lives of Marines that led then-Defense secretary Robert Gates to order a crash program to churn out 27,000 of the trucks, including an all-terrain version for Afghanistan.

The Pentagon says the trucks, featuring heavy armor and V-shaped hulls for deflecting blasts, saved thousands of lives.

About $2 billion was spent training troops in dealing with IEDs, with elaborate exercises involving actors, explosions and fake gore set up in the California desert at Fort Irwin to mimic combat in Iraq and Afghanistan.

Another $7 billion went for intelligence operations to dismantle networks financing, producing and placing IEDs.

Today in the twilight of American involvement in Afghanistan, commanders are cutting the chance of death by IED even further.

Missions to clear roads, among the last going "outside the wire," are pulling back to paved highways where burying bombs is harder. Clearance convoys are shadowed by Apache attack helicopters. Night missions, peripheral lights ablaze, look like roving football stadiums.

And bomb-defeating technology on board has reached a crescendo.

The trucks are wrapped in netting that can deflect rocket-propelled grenades. Inside, soldiers wearing helmets, body armor, protective goggles and fortified underwear sit on shock-absorbing seats and track potential IED hot spots on computer screens.

From inside their armored vehicles, they can remotely inspect and probe suspicious ground with long metal arms. They can deploy robots big and small. They have electronic jammers, ground-penetrating radar and giant IED-uncovering rakes.

"There's been some crazy devices that we're not even going to use," Spc. Crane says about the many inventions provided to them.

An Obama administration eager to put the IED chapter behind it has pledged to avoid long-term operations where the bombs are a threat. And as troops come home, the Pentagon is gradually turning much of its MRAP fleet in Afghanistan into scrap.

Staying alive

When Arizona National Guard engineers were clearing roads in Zabul province on Nov. 17, Staff Sgt. Alex Viola, 29, of Keller, Texas — a Green Beret on foot patrol in nearby Kandahar province advising Afghan troops — stepped on an IED and was killed.Four days earlier, another Green Beret — Staff Sgt.Richard Vazquez, 28, of Seguin, Texas — was killed by an IED on the same type of mission.

Afghan civilians and troops are now suffering the brunt of IED attacks. But the bombs still kill and

maim Americans, says Navy Capt. Dan Gramins, a vascular surgeon at a U.S. hospital in Kandahar, where a trickle of U.S. casualties from IEDs arrive each month.

It was at this facility that Army Cpl. Joshua Hargis, a Ranger who lost both legs to an IED blast on Oct. 6, delivered the "salute seen around the world" from his hospital bed after receiving a Purple Heart that later went viral.

If a soldier devastated by an IED can survive to reach a hospital, military doctors have become extremely proficient at saving them. "We're good at keeping them from dying," says Gramins. "But I think as long as we're fighting IEDs, we're going to continue to have multiple amputees."

The Arizona National Guard Army engineers will finish their 10-month deployment before Christmas. So there's a giddiness when a mission is over, as soldiers tumble out of their armored containers and bear-hug one another with exaggerated glee.

Inside the wire, they know where they step is safe.

"All of us know that when you go outside the wire," says Spec. Crane, "the threat is there."

*USA TODAY staff writer **Gregg Zoroya** covers the effect of war on troops and their families, and the problems Iraq and Afghanistan veterans face leaving the military for civilian life.*

North African Islamist terrorists dig up Nazi mines for use in IEDs

Source: http://www.homelandsecuritynewswire.com/dr20160815-north-african-islamist-terrorists-dig-up-nazi-mines-for-use-in-ieds

Aug 15 – **ISIS and its affiliate organization in North Africa have found a new source for munition materials: Digging up old landmines from the Second World War and using them to fashion IEDs for terrorist attacks.**

***Newsweek* reports that there are about seventeen million landmines buried in western Egypt and north-east Libya.**

Between 1940 and 1943 British and Commonwealth troops, under the command of Field Marshal Bernard Montgomery, fought pitched battles with Field Marshal Erwin Rommel's German army and his Italian allies for control of Egypt, Libya, and Tunisia.

Egyptian and NATO troops clearing mines in 2013.

The allied forces won a major victory in the second Battle of El Aalamein (23 October-4 November 1942), leading Winston Churchill famously to declare: "Now this is not the end [of the war]. It is not even the beginning of the end. But it is, perhaps, the end of the beginning."

The Germans and Italians withdrew from North Africa, but they left behind tons of munitions, which they buried beneath the Sahara Desert.
Egypt's landmine clearance chief, Fathy el-Shazly, told *Newsweek*: "We've had at least ten reports from the military of terrorists using old mines. Even now, these things trouble us in different ways."
El-Shazly said the Egyptian authorities first noticed the danger in 2004, when thirty-four people were killed in the resort of Taba, close to the border with Israel.
Forensic investigation confirmed that the seven bombs used in the Taba attack by an ISIS-affiliated, Sinai-based Islamist terror group had been fashioned from wartime munitions.
One group recycling and using the Nazi munitions is Ansar Beit al-Maqdis, which is based in Egypt's Sinai Desert and declared allegiance to ISIS in 2014.
The buried landmines continue to extract a toll even without the intervention of Islamist groups. Since 1945, about 7,000 Egyptians have been killed by mines in north-west Egypt. Since 2006, local Bedouin tribesmen have suffered 150 casualties.
It appears that ISIS and Ansar Beit al-Maqdis have found ways to retrieve and extricate the mines without setting them off, and then remove the explosives for use in making IEDs.
To address the growing terrorist threat, the Egyptian military has purchased 700 armored vehicles from the United States.
Military experts notes that Second World War-era weapons are used by different factions in the Middle East, not only by Islamist terrorists. Thus, one Syrian rebel group was found to be using 70-year-old howitzers.
N. R. Jenzen-Jones, an arms consultant, told *Newsweek*: "We've seen several dozen British Webley revolvers previously or presently for sale, and then some Italian cavalry carbines, some Mausers, Bren guns.'

EDITOR'S COMMENT: This is a very serious info that should be taken into account in Europe. Especially in Central Europe where there are still chemical munitions abandoned in the fields of WWI. Some might still contain quantities of sulphur mustard enough to assemble a chemical dispersal device.

'Threat of terrorism' sparks call to reopen Canada bomb center

Source: https://www.yahoo.com/news/threat-terrorism-sparks-call-reopen-canada-bomb-center-171754652.html

Aug 14 – Days after police foiled what they called a terrorist plot, a Canadian law enforcement body was preparing to make the case for reopening the federal bomb analysis center, which was shut in April for budget reasons.

The Calgary Police Commission was expected to make its case for the Canadian Bomb Data Centre in a resolution at the Canadian Association of Police Governance annual general meeting on Sunday.
The event comes three days after police say an alleged Islamic State supporter detonated an explosive device and was killed in a raid in the province of Ontario.
The resolution, by the police oversight body from the city of Calgary, Alberta, did not mention the Ontario incident. But it said the center had been a valuable tool and was all the more necessary now.
"Terrorism and the threat of terrorism is increasing both domestically and abroad, making it incumbent upon governments and law enforcement agencies to amplify rather than diminish efforts," read the resolution.
If passed by the association, which comprises municipal police boards and commissions, the resolution is not expected to be binding on the federal police force that ran the center.

It instead "urges the federal government to restore funding that will permit the Canadian Bomb Data Centre to continue its operation."

According to the Royal Canadian Mounted Police (RCMP) federal agency, the center analyzed bomb data and how to handle explosives and provided assistance and coordination to police forces dealing with the matter.

"Individual police agencies are now responsible for collecting and storing their own data" and do not have the same level of coordination and expertise as before, the resolution read.

Canada recorded a big jump in terrorism offences last year with 173 alleged incidents, up from 76 in 2014, according to July data from Statistics Canada, which cites police information.

In October 2014, a Canadian Muslim convert shot and killed a soldier at Ottawa's national war memorial before launching an attack on the Canadian Parliament. The same week, another convert ran down two soldiers in Quebec, killing one.

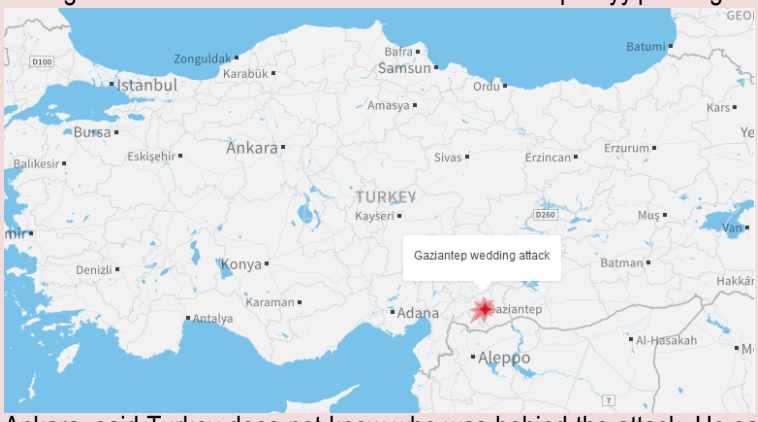
The RCMP did not immediately respond to a request for comment.

Turkey backtracks on age of wedding bomber

Source: http://edition.cnn.com/2016/08/22/asia/turkey-gaziantep-blast/index.html

Aug 23 – The Turkish government is now backtracking on its initial claim that the attacker who bombed the Kurdish wedding celebration in southern Turkey on Saturday night was a young teenager.

The **bombing killed 54 people in Gaziantep** near the Syrian border and it stunned Turks -- not just for the high death toll but also because President Recep Tayyip Erdogan said on Sunday that **the bomber was between 12 and 14 years old.**



ISIS, which has used children in combat or to act as human bombs in attacks across the Middle East, is suspected in the attack, Erdogan said. No group has claimed responsibility for the blast.

On Monday, Prime Minister Binali Yildirim, speaking to reporters in the capital of Ankara, said Turkey does not know who was behind the attack. He said it's unclear at the present time whether the attacker was "a child or an adult."

It is rumored that the attacker was a child, Yildirim said.

"The security forces are focusing on it and trying to find clues related to it," the prime minister said.

Many of those killed were young teens

Twenty-two of the 54 killed in a devastating bomb attack that struck the wedding were under 14, a Turkish official said Monday.

The revelation added a fresh layer of horror to the bombing, which also wounded dozens of others. It was the deadliest in a string of blasts across Turkey this year.

The bomb struck in crowded streets of the Beybahce neighborhood of Gaziantep's Sahinbey district during celebrations for the wedding of a Kurdish couple.

The blast disproportionately killed women and children, as it had been timed to detonate during a part of the festivities when those groups painted themselves with henna, authorities said.

As the dead were swiftly laid to rest, in accordance with Islamic tradition, their loved ones spoke of their anguish.

Emine Ayhan, who lost four of her five children and whose husband was seriously injured, told Turkish television: "If my remaining child was not alive, I would commit suicide."

Hakki Okur, 14, was among the young victims. His cousin, Mesut Bozkurt, recounted searching for the teen throughout the night following the blast before his family was summoned to the hospital to identify his body.

"No injuries on his head, but burns on his chest," Bozkurt said.
"We think he may have been trapped in the panic since he was a skinny boy."

ISIS has a strong presence in Gaziantep

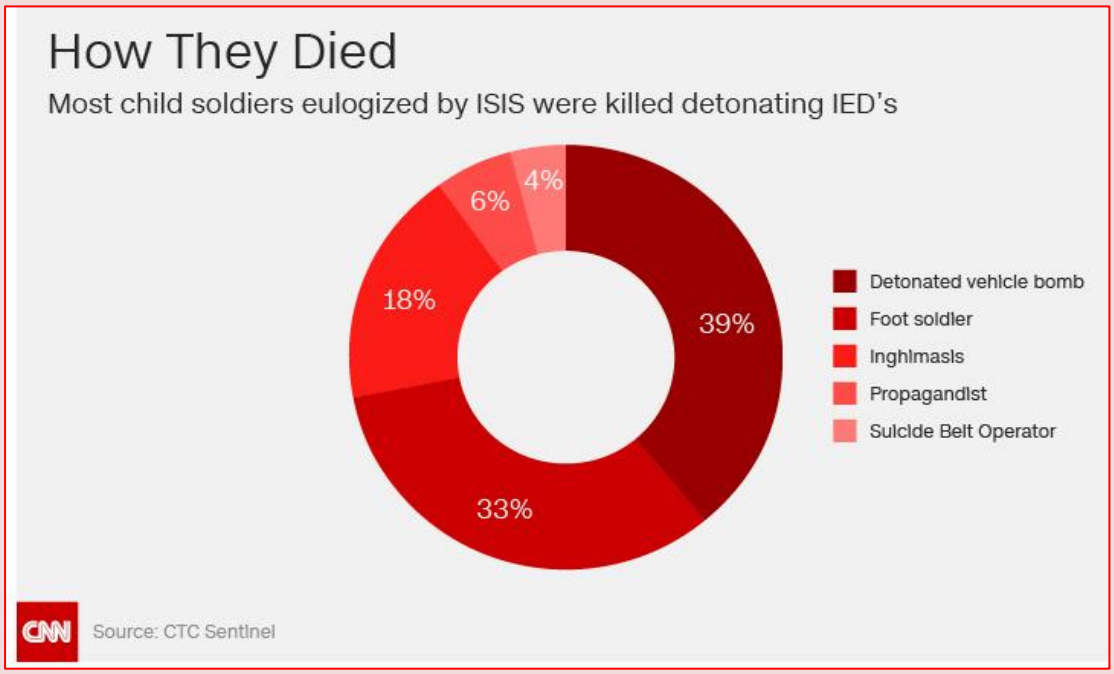
Authorities found remnants of an explosive vest at the scene, and officials said they are not clear whether it was detonated remotely or by the bomber.
ISIS, which has struck before in Gaziantep and reportedly has a strong presence in the city, traditionally hasn't claimed responsibility for attacks on Turkish soil.
Gaziantep is about 95 kilometers (60 miles) north of the war-torn Syrian city of Aleppo.

Child bomber thwarted in Iraq

On Sunday, a would-be child bomber was captured by security guards in Kirkuk -- a city in northern Iraq with a large Kurdish population. Broadcaster Kurdistan 24 aired footage of guards apprehending the teen and stripping him of his suicide vest before he could strike.

Watch the video at:
https://www.youtube.com/watch?v=2asr9XBaz24

Najmaldin Karim, the governor of Kirkuk province, told CNN that the thwarted bomber was a 15-year-old who arrived from Mosul -- the largest city under ISIS control -- a week earlier. Following an earlier suicide attack in the city Sunday, the guards noticed something odd about the teen and stopped him before he struck his target, a Shia mosque.
"He is trained and brainwashed," Karim told CNN.
"They tell them if they do this, they will go to heaven and have a good time and get everything that they ever wanted."



Mia Bloom, a Georgia State University professor who is an expert on child soldiers and terrorism, said ISIS made wide use of children in conflict, typically employing them as bombers or snipers, either attached to adult fighting units or operating on their own.
The organization has eulogized more than 250 child attackers on its channels on Telegram, an encrypted messaging app the terror group widely uses.
ISIS has lured children "through a variety of tricks and treats, the way pedophiles lure in young kids," she said.

But often -- if child soldiers are internally displaced persons, as the thwarted Kirkuk bomber was reported to be, or otherwise vulnerable -- they may feel "that they had no choice but to join ... perhaps in exchange for food or protection or not upsetting the authorities in Raqqa or in Mosul."
Child bombers who are coerced often deliberately fail to launch their attacks, as the teen in Kirkuk may have done, she said.

EDITOR'S COMMENT: His brother detonated himself one hour before boy's arrest near a Shiite mosque injuring two people. Their father seemed to be the person orchestrating both attacks…

DNC hack: "All roads lead to Russia" says new cybersecurity report

Source: http://www.homelandsecuritynewswire.com/dr20160727-dnc-hack-all-roads-lead-to-russia-says-new-cybersecurity-report

July 27 – New report by a cybersecurity firm ThreatConnect focuses on Guccifer 2.0, a hacker claiming to be behind the hack of the DNC computer system. The claim was made in order to deflect attention from Russian government hackers whose digital fingerprints were all over the DNC hack. A ThreatConnet report shows that **Guccifer 2.0 is part of the Russian plot to steal and release politically embarrassing DNC e-mails.**

On Monday we reported that cybersecurity experts agreed with Robby Mook, Hillary Clinton's campaign manager, that the WikiLeaks release on Friday of politically sensitive Democratic National Committee (DNC), e-mails which were embarrassing to the Clinton campaign, was the work of Russian government hackers ("Russian government hackers leaked DNC e-mails: Cybersecurity experts," HSNW, 25 July 2016).

Patrick Tucker, writing in *Defense One*, notedthat an individual going by the moniker Guccifer 2.0 claimed that he was the hacker who broke into the DNC systems and gave the e-mails to WikiLeaks.

Cybersecurity firm CrowdStrike, which was among the first to report of the Russian government's hacking campaign against American organizations, said that Guccifer 2.0's claims notwithstanding, they were confident in their analysis: "These claims do nothing to lessen our findings relating to the Russian government's involvement, portions of which we have documented for the public and the greater security community."

Other cybersecurity firms looking at the data reached the same conclusions CrowdStrike reached (see the analysis by Dan Goodin in *Ars Technoca*, and by Lorenzo Franceschi-Bicchierai in *Motherboard*).

Security experts note that the very intervention by Guccifer 2.0 lends support to the conclusion that Russian government hackers were behind the hacking of the DNC systems: Russian intelligence often throws a smoke-screen around its operations by creating actors who take responsibility for certain operations, or "eye witnesses" who offer "evidence" supporting the Russian version of events.

On Tuesday, cybersecurity firm ThreatConnect issued a detailed, comprehensive report, using its own data and data from earlier by cybersecurity firms CrowdStrike, Mandiant, and Fidelis – a report which definitely shows that Russian government hackers, working under the names Fancy Bear and Cozy Bear, hacked the computer systems of the DNC.

In the report, titled, "Guccifer 2.0: All Roads Lead to Russia," ThreatConnect's researchers write:

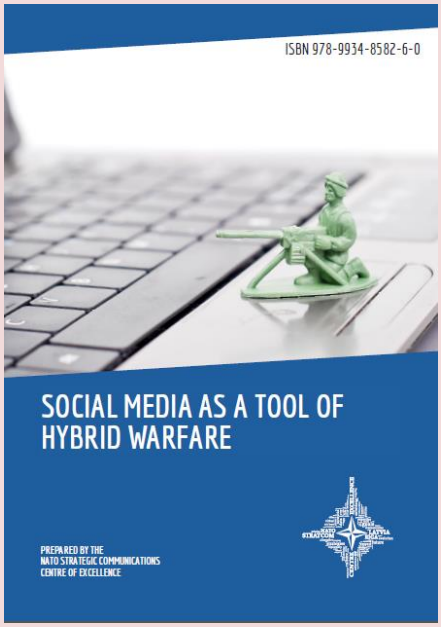
> *In our initial Guccifer 2.0 analysis, ThreatConnect highlighted technical and non-technical inconsistencies in the purported DNC hacker's story as well as a curious theme of French "*connections*" surrounding various Guccifer 2.0 interactions with the media. We called out these connections as they overlapped, albeit minimally, with FANCY BEAR infrastructure identified in CrowdStrike's DNC report.*
>
> *Now, after further investigation, we can confirm that Guccifer 2.0 is using the Russia-based Elite VPN service to communicate and leak documents directly with the media. We reached this conclusion by analyzing the infrastructure associated with an email exchange with Guccifer 2.0 shared with ThreatConnect by* Vocativ's *Senior Privacy and Security reporter Kevin Collier. This discovery strengthens our ongoing assessment that Guccifer 2.0 is a Russian propaganda effort and not an independent actor.*

Note that the ThreatConnect report assumes a certain level of computer-technical knowledge on the part of the reader. For an accessible summary of the report, and a conversation with Kevin Collier, see Sam Thielman, "DNC email leak: Russian hackers Cozy Bear and Fancy Bear behind breach," *Guardian* (26 July 2016).

Social media as a tool of hybrid warfare

Source: http://www.stratcomcoe.org/social-media-tool-hybrid-warfare

The development of information technology has changed the nature of conflicts by creating an additional layer of complexity to traditional battle spaces. Nearly global access to the virtual environment has created numerous opportunities to conduct battles online affecting events in both the physical domain, such as computer systems, and in the cognitive domain of people's attitudes and beliefs.



Recently we have witnessed how both states and non-state actors use hybrid approaches to pursue their political and military aims, skilfully combining military operations with cyber-attacks, diplomatic and/or economic pressure, and information (propaganda) campaigns. Over the past decade, social media has rapidly grown into one of the main channels of communication used today. Virtual communication platforms have become an integral part of warfare strategy. The recent conflicts in Libya, Syria, and Ukraine have demonstrated that social media is widely used to coordinate actions, collect information, and, most importantly, to influence the beliefs and attitudes of target audiences, even mobilise them for action.

Given this state of affairs, the NATO Strategic Communications Centre of Excellence (NATO StratCom COE) was tasked with looking into how state and non-state actors leverage social media as a tool for conflict and hybrid warfare strategies. The following topics will be addressed in the report:

- What is the role of social media in hybrid warfare? How is it 'weaponised'?
- What techniques and tactics do state and non-state actors employ to support their political and military aims using social media? What effects can they achieve?
- What can NATO and its member nations do to identify and counter the malicious use of social media?

We hope that this paper will serve as a comprehensive introduction and useful educational material for anyone interested in understanding the complexity of today's information environment, and specifically the techniques of influence used in the digital space.

The report summarises the conclusions of research commissioned by the StratCom COE—*Internet trolling as hybrid warfare tool: the case of Latvia* by the Latvian Institute of International Affairs (LIIA) in cooperation with Riga Stradiņš University,1 *Social influence in Russia-Ukraine-conflict-related communication in social media* by a team of Polish researchers,2 *Network of terror: how Daesh uses adaptive social networks to spread its message* by Joseph Shaheen, US State Department Fellow at the StratCom COE, as well as discussions from the seminars and conferences conducted by the COE over the course of 2015.

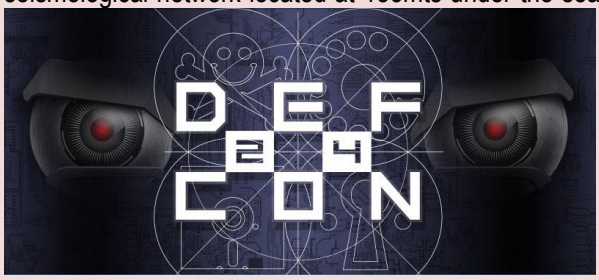
The StratCom COE would like to thank Thomas Elkjer Nissen, Head of the StratCom Section of the Royal Danish Defence College, Dr Rebecca Goolsby, Project Officer at the US Office of Naval Research, Col (rtd) Ian Tunnicliffe, Director of Accordance Associates, Prof Aki-Mauri Huhtinen, Professor of Military Leadership and Management at the Finnish National Defence University, Prof Ben O'Loughlin, Professor of International Relations at the Royal Holloway University of London, Nik Gowing, Visiting Professor in War Studies at Kings College London, Assoc prof Cristina Archetti, Lecturer at the University of Oslo, as well as Mark Laity, Chief of Strategic Communications at NATO SHAPE, for valuable contributions to the social media related discussions organised by the StratCom COE.

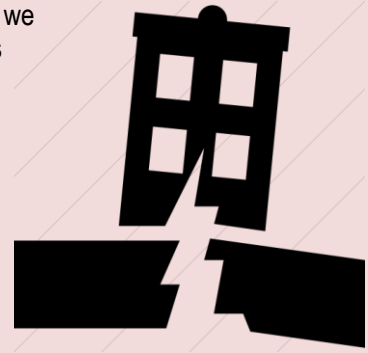
▶ **You can read the full report at source's URL.**

Exploiting and Attacking Seismological Networks... Remotely

By Bertin Bervis Bonilla Founder and James Jara
Source: https://www.defcon.org/html/defcon-24/dc-24-speakers.html#Bonilla

Aug 08 – In this presentation we are going to explain and demonstrate step by step in a real attack scenario how a remote attacker could elevate privileges in order to take control remotely in a production seismological network located at 183mts under the sea. We found several seismographs in production connected to the public internet providing graphs and data to anyone who connects to the embed web server running at port 80. The seismographs provide real time data based in the perturbations from earth and surroundings, we consider this as a critical infrastructure and is clear the lack of protection and implementation by the technicians in charge.





We are going to present 3 ways to exploit the seismograph which is segmented in 3 parts: Modem (GSM, Wi-Fi, Satellite, GPS,Com serial) {web server running at port 80 , ssh daemon} Sensor (Device collecting the data from ground or ocean bottom) Battery (1 year lifetime) Apollo server (MAIN acquisition core server) These vulnerabilities affect the Modem which is directly connected to the sensor , a remote connection to the modem it's all that you need to compromise the whole seismograph network. After got the root shell our goal is execute a post exploitation attack , This specific attack corrupts/modifies the whole seismological research data of a country/ area in real time. We are going to propose recommendations and best practices based on how to deploy a seismological network in order to avoid this nasty attacks.

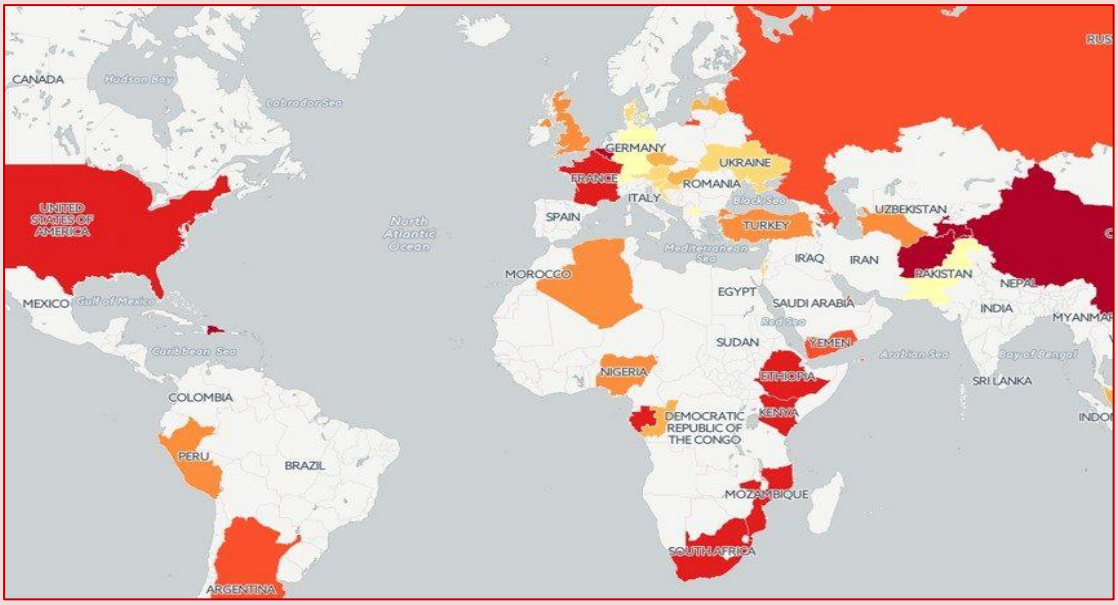
Bertin Bervis Bonilla *is a security researcher focused in offensive security, reverse engineering and network attacks and defense, Bertin has been speaker in several security conferences in his country and latin america such OWASP Latin Tour , DragonJAR conference and EKOPARTY, He is the founder of NetDB - The Network Database project , a computer fingerprint/certificate driven search engine. Formerly is a network engineer working for a five letters us networking company in San Jose Costa Rica.* ***James Jara*** *is the founder and CTO of NETDB.IO , a search engine of internet of things focused in info-security research. He likes Bitcoin Industry, Open Source and framework development and gave various presentations on security conferences like EkoParty. Interested machine learning for mobile, Internet of Things (IoT) devices and industrial systems used in critical infrastructure networks. Sport-coder!*

The countries most vulnerable to cyber-attacks

Source: http://www.telegraph.co.uk/technology/2016/06/10/mapped-the-countries-most-vulnerable-to-cyber-attacks/

June 10 – A security company has identified and ranked the 50 countries most vulnerable to hacking, based on the prevalence of insecure networks and internet channels around the world.
Rapid7 found that Belgium was the most susceptible country based on a "National Exposure Index" of unsafe or potentially vulnerable internet services. The UK was ranked 23rd most exposed, the US 14th and Australia 4th.
Rapid7's Project Sonar software scans millions of internet channels for vulnerabilities such as unencrypted, plain text services, and by comparing this to more secure ones, can determine the chances of coming across an at-risk channel.

Channels that are not encrypted are not necessarily passing sensitive data, but many are likely to be, so their prevalence at a national level is a good indicator of how secure the internet is in each country. By identifying vulnerabilities at the IP address level, the researchers were able to identify what country they are in.



Rapid7 warned that the world's biggest economies would face "dire consequences" if the current state of affairs continued, as the rise of the internet of things creates billions of new connections.

The vulnerabilities measured by Project Sonar included out-of-date email encryption and server ports that expose databases directly to the internet rather than being locked. **In Belgium's case, 31 per cent of systems or devices had at least 30 ports exposed. Unencrypted ports mean people snooping on a network can possibly gain access to private information.**

"In the days when the internet was a shared resource among a very few academic and military institutions, exposing databases and connecting directly to them across the internet made some sense," the report's authors said. "However, even in a case where encryption and strong authentication is possible, exposing a database directly to the **3.5 billion human internet population** is no longer a sensible act.

"These results all speak to a fundamental failure in modern internet engineering. Despite calls from the Internet Architecture Board, the Internet Engineering Task Force, and virtually every security company and security advocacy organization on Earth, compulsory encryption is not a default, standard feature in internet protocol design."

The most vulnerable countries

1. Belgium
2. Tajikistan
3. Samoa
4. Australia
5. China
6. Hong Kong
7. Dominican Republic
8. Afghanistan
9. South Africa
10. Ethiopia
11. Kenya
12. Gabon
13. France
14. United States
15. Mozambique
16. Japan
17. Qatar
18. Yemen
19. Russia
20. Argentina
21. Maldives
22. Azerbaijan
23. United Kingdom
24. Turkmenistan
25. Algeria
26. South Korea
27. Peru
28. Nigeria
29. Turkey
30. Hungary
31. Malaysia
32. Congo
33. Taiwan
34. Czech Republic
35. Bahamas
36. Latvia
37. Ukraine
38. Slovenia
39. Austria
40. Croatia
41. Denmark
42. Luxembourg
43. Israel
44. Macedonia
45. Pakistan
46. Cyprus
47. Germany
48. Switzerland
49. Singapore
50. Vietnam

The First Weapon Against Lone Terrorists: Big Data Analytics

By Yaakov Lappin

Source: http://www.breitbart.com/jihad/2016/08/05/first-weapon-lone-terrorists-big-data-analytics/

Aug 05 – European security and intelligence agencies are scrambling to regroup and reorganize following a steady, growing flow of jihadist atrocities. They have a steep learning curve ahead of them when it comes to thwarting terrorism.

To do so, European governments will need to greatly expand budgets for domestic and overseas intelligence operations, create international security cooperation, and enable real-time intelligence sharing, on a scale not seen before. They will also need to deploy wide-reaching signals intelligence capabilities that will build up a database of leads, for monitoring and arresting suspects. Such tactics work very well against transnational terror networks which involve ISIS command centers in Syria and Iraq dispatching cells to the West, or with localized cells in Western cities acting under the influence of ISIS ideology.

Yet even a country like Israel, which arguably has the biggest scope of counter-terrorism experience on Earth, has not been able to prevent a different type of terrorism, which led to a succession of Palestinian attacks that began last year. In most cases, alert security forces and members of the public responded quickly to neutralize the attackers, but the fact remains that Israel's vaunted intelligence services had not been able to thwart these attacks, and for good reason.

The vast majority of "successful" terrorism that got through Israel's security net is of the "lone-wolf" kind. These are Palestinian attackers who woke up one morning, and, influenced by a potent concoction of jihadist incitement to violence and personal triggers, decided that would be the day that they open fire, run over, or stab their victims and die in the process.

The organized kind of terrorism has reared its head rarely in Israel in recent months and years, due to the nightly arrests and 24-7 intelligence-gathering work that thwarts these threats, and prevents Israeli cities from turning into perpetual war zones.

Organized terrorist cells leave behind tracks, such as instructions via phone calls or internet communications, the transfer of money, suspicious purchases of chemicals and weapons, and other warnings signals that can be picked up by a well-funded, hi-tech national intelligence agency with good human intelligence coverage on the ground too.

The lone attacker, on the other hand, does not usually communicate with others and can easily move under the radar of national security forces, at least until now.

Israeli security officials have begun employing a new weapon in the war against lone attackers: Big data analytics. This new counter-terrorism measure could prove to be equally useful and life saving in the West, where cities are increasingly being attacked by lone terrorists inspired by ISIS's murderous ideology.

Although it is still under development, Israel's Shin Bet domestic intelligence agency and other security groups have begun using advanced algorithms to sift through a vast volume of social media activity. Their goal is to search for the small – yet deadly – needles in a haystack of online information, and find warning signs pointing to an individual who is primed to strike.

The old thinking, that lone attackers do not communicate with others, may have been wrong, it turns out. They may, in fact, be communicating with the entire world through social media, and if anyone cares to listen to them attentively enough, their murderous intentions might be foiled. The precise details of this technique remain classified, but it is being used on an increasing basis by Israeli security agencies monitoring Palestinian threats.

The internet remains the prime recruitment tool used by ISIS to convert Muslims in Europe into terrorists, and ISIS has expressed a preference for those keen on carrying out acts of jihad to do so on their Western home turf, rather than travel to the caliphate.

Within Israel's battle against Palestinian terrorism, big data analytics have begun to work, and for the first time, a number of lone attackers were arrested before they could pounce, according to security sources.

Security forces have recently issued warnings to individuals marked as potential future lone attackers, making clear the

repercussions of such acts on their families. After terror attacks, the government of Israel often orders the army to demolish the home of the perpetrators.

The number of lone attackers has decreased in recent months for a variety of reasons, and big data countermeasures appear to be among them.

Security forces have begun monitoring Facebook pages of young people who have praised past acts of murder and express desire to become martyrs. Most of those who express jihadist sentiments do not go on to the action stage, but a minority of suspects do, and the correct algorithms can help identify them.

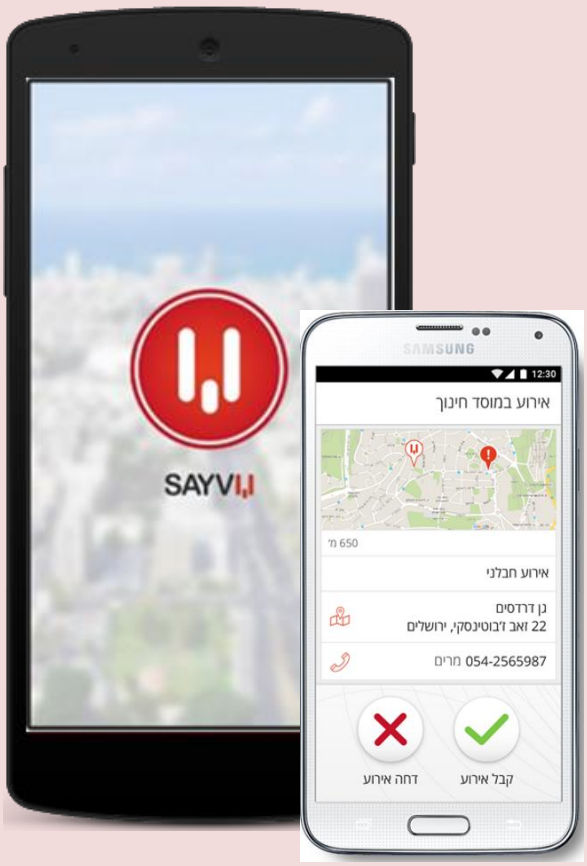
The system remains far from perfect, and security sources say much more work is needed to improve results. It is, however, the first time that technology is being used not only to break up budding, organized terrorism cells, but also to track down and arrest the lone wolves before they pounce.

***Yaakov Lappin** is the Jerusalem Post's military and national security affairs correspondent, and author of The Virtual Caliphate (Potomac Books, 2011), which proposes that jihadis on the internet established a virtual Islamist state and sought to upload it in failed states. The book was published four years before ISIS declared a caliphate.*

SayVU security app – developed by a BGU graduate student -- deployed at Rio Olympics

Source: http://www.homelandsecuritynewswire.com/dr20160809-sayvu-security-app-developed-by-a-bgu-graduate-student-deployed-at-rio-olympics

Aug 09 – A new app, SayVU, conceived as a graduate student project at Ben-Gurion University of the Negev, is being deployed at the 2016 Rio Olympics. International Security & Defense Systems (ISDS), the security integrator for the Olympics, selected SayVU as one of the Israeli technologies being used to protect attendees.



SayVU, now available on the Android platform, enables a user to send a distress signal to an emergency hotline even if a phone is locked and without having to access the application. The message can be sent in a number of ways; shaking the device, tapping the camera button, or simply speaking into the phone.

"SayVU strives to minimize the response time of emergency services and other authorities, and make sure the user gets assistance as quickly as possible," according to SayVU CEO Amotz Koskas. "We have established a hotline center at the 2016 Rio Olympics, which help emergency and law enforcement agencies respond to alerts and ensure the safety of Olympics attendees."

SayVU also includes the option for automatically turning on the phone's microphone. It sends the recorded voice, GPS, and other locating information to an emergency hotline. The app uses patent pending machine learning techniques to determine the user's patterns and checks when it senses abnormalities. If there is no reply, the app automatically sends out a distress message.

In addition to SayVU's lifesaving security benefits, the technology provides real-time event and emergency reporting to emergency medical services (EMS) and law enforcement agencies as well as

threat management, regional threat mapping and trend prediction.

The American Associates, Ben-Gurion University of the Negev (AABGU) notes that the technology was conceived and developed in the wake of the kidnapping and murder of three Israeli youths in 2014. One of them managed to call and report the kidnapping, but the police did not immediately respond because they thought it was a prank call. Koskas, at the time an MBA student at BGU's Guilford Glazer Faculty of Business and Management, wondered whether there was a technological means to prevent similar instances in the future.

A year later, Koskas won the joint Google and BGU competition "Students Thinking Innovation in the Public Sector" in collaboration with "Digital Israel" and the staff of the "Accessible Government" initiative to promote innovation in the public sector through information and communication technologies. The new technology attempted to meet two main needs: to give citizens the tools to send out a distress message and location quickly in an emergency, and to enable the authorities to get a clear, real-time situation report.

Recently, the company ran a pilot with kindergartens in Ofakim, Israel. It was deemed a success when a pedophile was caught by a teacher who used the app. As a result, the Ofakim municipality decided to use the app for all educational institutions, social workers, and the municipal hotline, with other municipalities following suit.

SayVU Ltd. has embarked on a $2 million round of funding. The company is developing strategic partnerships in the United States, China, Europe, and Africa.

AABGU notes that the company was also just awarded a $1 million grant from the U.S.-Israeli BIRD Foundation for a project funded by Israel's Public Security Ministry and the U.S. Department of Homeland Security. **The goal is to provide orientation within buildings and non-failure communications under extreme conditions to first responders such as police, firefighters, and emergency medicine personnel.**

If two countries waged cyber war on each another, here's what to expect

By Bill Buchanan

Source: http://www.homelandsecuritynewswire.com/dr20160809-if-two-countries-waged-cyber-war-on-each-another-here-s-what-to-expect

Aug 09 – Imagine you woke up to discover a massive cyberattack on your country. All government data has been destroyed, taking out healthcare records, birth certificates, social care records and so much more. The transport system isn't working, traffic lights are blank, immigration is in chaos, and all tax records have disappeared. The Internet has been reduced to an error message and daily life as you know it has halted.

This might sound fanciful but don't be so sure. When countries declare war on one another in future, this sort of disaster might be the opportunity the enemy is looking for. The Internet has brought us many great things but it has made us more vulnerable. Protecting against such futuristic violence is one of the key challenges of the twenty-first century.

Strategists know that the most fragile part of Internet infrastructure is the energy supply. The starting point in serious cyber warfare may well be to trip the power stations which power the data centers involved with the core routing elements of the network.

Back-up generators and uninterruptible power supplies might offer protection, but they don't always work and can potentially be hacked. In any case, backup power is usually designed to shut off after a few hours. That is enough time to correct a normal fault, but cyberattacks might require backup for days or even weeks.

William Cohen, the former U.S secretary of defense, recently predicted such a major outage would cause large-scale economic damage and civil unrest throughout a country. In a war situation, this could be enough to bring about defeat. Janet Napolitano, a former secretary at the Department of Homeland Security, believes the American system is not well enough protected to avoid this.

Denial of service

An attack on the national grid could involve what is called a distributed denial of service (DDoS) attack. These use multiple computers to flood a system with information from many sources at the same time. This could make it easier for hackers to neutralize the backup power and tripping the system.

DDoS attacks are also a major threat in their own right. They could overload the main network gateways of a country and cause major outages. Such attacks are commonplace against the private sector, particularly finance companies. Akamai Technologies, which controls 30 percent of Internet traffic, recently said these are the most worrying kind of attack and becoming ever more sophisticated.

Akamai recently monitored a sustained attack against a media outlet of 363 gigabits per second (Gbps) – a scale which few companies, let alone a nation, could cope with for long. Networks specialist Verisign reports a shocking 111 percent increase in DDoS attacks per year, almost half of them over 10 Gbps in scale – much more powerful than previously. The top sources are Vietnam, Brazil, and Colombia.

Most DDoS attacks swamp an internal network with traffic via the DNS and NTP servers that provide most core services within the network. Without DNS the Internet wouldn't work, but it is weak from a security point of view. Specialists have been trying to come up with a solution, but building security into these servers to recognise DDoS attacks appears to mean re-engineering the entire Internet.

How to react

If a country's grid were taken down by an attack for any length of time, the ensuing chaos would potentially be enough to win a war outright. If instead its online infrastructure were substantially compromised by a DDoS attack, the response would probably go like this:

Phase one: Takeover of network: the country's security operations center would need to take control of Internet traffic to stop its citizens from crashing the internal infrastructure. We possibly saw this in the failed Turkish coup a few weeks ago, where YouTube and social media went completely offline inside the country.

Phase two: Analysis of attack: security analysts would be trying to figure out how to cope with the attack without affecting the internal operation of the network.

Phase three: Observation and large-scale control: the authorities would be faced with countless alerts about system crashes and problems. The challenge would be to ensure only key alerts reached the analysts trying to overcome the problems before the infrastructure collapsed. A key focus would be ensuring military, transport, energy, health and law enforcement systems were given the highest priority, along with financial systems.

Phase four: Observation and fine control: by this stage there would be some stability and the attention could turn to lesser but important alerts regarding things like financial and commercial interests.

Phase five: Coping and restoring: this would be about restoring normality and trying to recover damaged systems. The challenge would be to reach this phase as quickly as possible with the least sustained damage.

State of play

If even the security-heavy United States is concerned about its grid,

the same is likely to be true of most countries. I suspect many countries are not well drilled to cope with sustained DDoS, especially given the fundamental weaknesses in DNS servers. Small countries are particularly at risk because they often depend on infrastructure that reaches a central point in a larger country nearby.

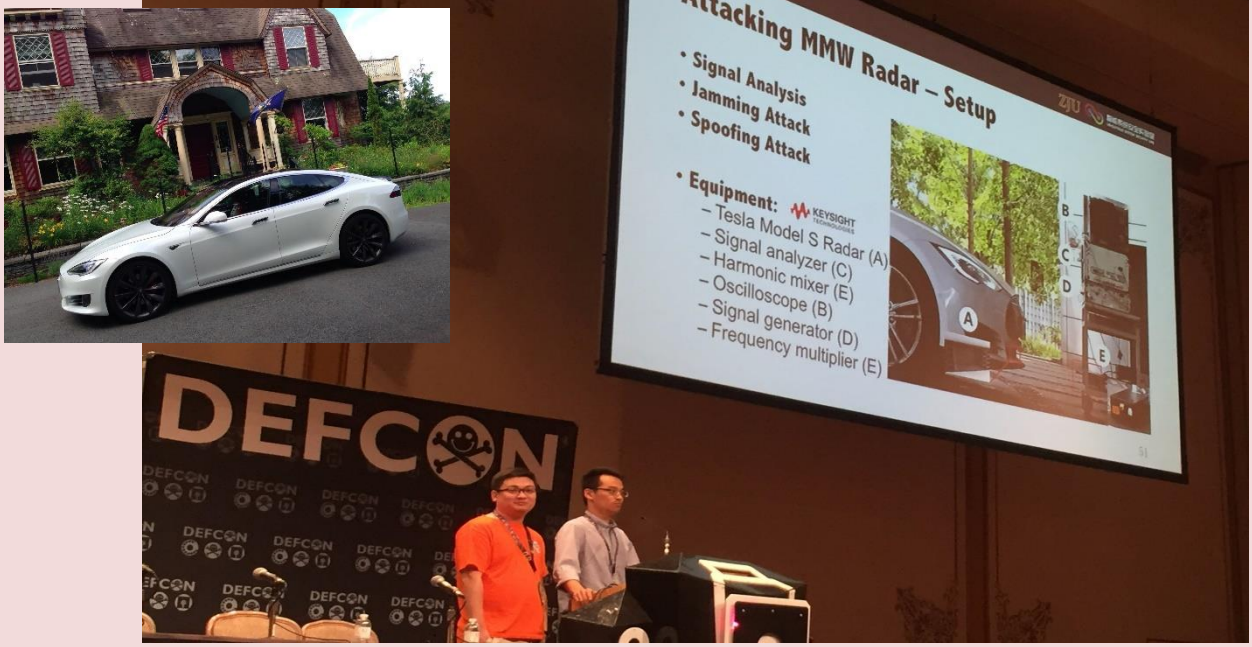
The United Kingdom, it should be said, is probably better placed than some countries to survive cyber warfare. It enjoys an independent grid and GCHQ and the National Crime Agency have helped to encourage some of the best private sector security operations centers in the world. Many countries could probably learn a great deal from it. Estonia, whose infrastructure was disabled for several days in 2007 following a cyberattack, is now looking at moving copies of government data to the United Kingdom for protection.

Given the current level of international tension and the potential damage from a major cyberattack, this is an area that all countries need to take very seriously. Better to do it now rather than waiting until one country pays the price. For better and worse, the world has never been so connected.

Bill Buchanan *is Head, The Cyber Academy, Edinburgh Napier University.*

Hackers show how they tricked a Tesla into hitting objects in its path

Source: http://uk.businessinsider.com/defcon-tesla-jamming-spoofing-autopilot-2016-8?r=US&IR=T



Aug 08 – **A group of researchers presenting at last week's Def Con hacker conference showed how they were able to overwhelm or deceive Tesla's sophisticated sensors to make a car hit an object it would normally detect in its path.**

"Normally the car will not move. However, when we jam the sensor it moves," Chen Yan said in a talk on Friday while playing a demo video of a Tesla Model S attack.

"It hit me," he added, to audience laughter.

It's important to note that the demonstration was a proof-of-concept that did not mimic real-world conditions today. Researchers were working on cars that were usually stationary with what was sometimes very expensive equipment. They noted that the "sky wasn't falling."

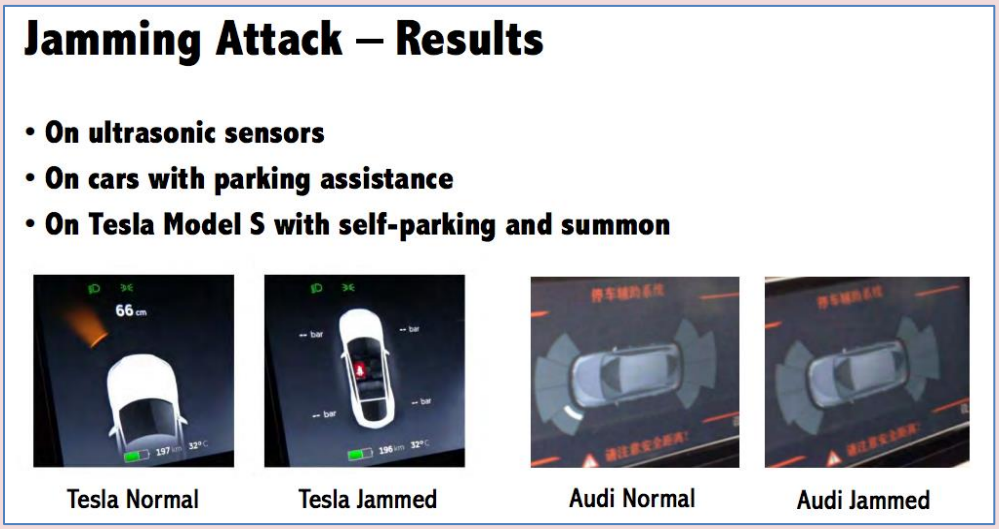
But the experiment suggests that theoretically, a few years from now, somebody could make a device that could jam certain sensors in a nearby car.

The group, which consisted of Chen Yan, a PhD student at Zhejiang University, Jianhao Liu, a senior security consultant at Qihoo 360, and Wenyuan Xu, a professor at Zhejiang

University and The University of South Carolina, presented a variety of new findings. They discovered methods for "quieting" sensors to diminish or hide obstacles in a car's path, "spoofing" them to make an object appear farther or closer than it actually is, and jamming, which, Yan said, renders the sensor useless as it's "overwhelmed by noise."

"This is definitely interesting and good work," Jonathan Petit, the principal scientist at Security Innovations, who has also presented research on deceiving autonomous vehicles, told Wired. "They need to do a bit more work to see if it would actually collide into an object. You can't yet say the Autopilot doesn't work."

There are a number of sensors on a Tesla Model S that are used for a variety of functions. It has radar to detect objects in front of it, GPS for location tracking, and cameras to detect speed limit signs and lane markings, for example. As the talk showed, many of these things can be tricked by a determined attacker.



"What would happen if there is an intentional malicious attacker?" asked Liu.

Much of their presentation focused on the Tesla Model S, but they also successfully jammed sensors on cars from Audi, Volkswagen, and Ford.

In a video demonstrating an attack, the researchers jammed sensors in the rear of the Model S, so the car did not know it was about to hit a person standing behind it. In another, they "spoofed" its Autopilot to trick it into thinking it would drive into something that was not actually there.

They also used off-the-shelf lasers to defeat the onboard cameras, and, in one of the most low-tech demonstrations, they wrapped objects up in cheap black foam that rendered them invisible to the car's sensors.

"[It was the] same effect as jamming," said Yan. He told Business Insider after the talk that Tesla reacted positively when they disclosed their research, and it was researching ways to mitigate these types of attacks.

"They appreciated our work and are looking into this issue," he said.

▶ **The full presentation of their findings is** available at Def Con's website.

Hackers target World Anti-Doping Agency, sports court

Source: http://arizonasports.com/story/775766/hackers-target-world-anti-doping-agency-sports-court/

Aug 11 – **The World Anti-Doping Agency and Court of Arbitration for Sport say they have been targeted by hackers, with an attempt made to obtain access credentials for the database which tracks athletes for drug testing.**

WADA said it learned "this week," during the Olympics, that it had been targeted, though it was not immediately clear when the attacks took place.

WADA communications coordinator Maggie Durand told The Associated Press in an email that the agency was notified of a YouTube video claiming WADA's website had been hacked. She says an investigation "was quickly able to determine that the website had not been

compromised, although we continue to monitor activity."

Durand says WADA's ADAMS database of doping results "has not been compromised," but that so-called phishing emails were sent to users of the database disguised as official WADA communications requesting their login details.

WADA did not immediately respond to requests for comment on how many users were targeted by the e-mails, whether athletes had been targeted, or what WADA's plan was if credentials had been leaked. WADA said it had notified all users of the database about the phishing attempt, and posted a warning on the database website.

Athletes use the database to enter so-called "whereabouts" information which they are obliged to provide in order to make themselves available for drug testing outside competitions. Someone with an athlete's credentials could potentially change that information, sending testers to the wrong location, potentially leading to athletes being wrongly blamed for missing a test.

Meanwhile, CAS secretary general Matthieu Reeb told the AP "there has been an attempt to hack the CAS website. It is not the first time, and certainly not the last time."

He says the attempt "was apparently unsuccessful but investigations are being made … to make sure that we have not suffered any damage."

Reeb says information on the CAS website "is intended for the public and is not confidential."

A video posted to YouTube, by a user claiming to represent Polish hackers, seems to show the CAS website doctored to display the message: "We forgot the sport is out of the politic (sic). Please forgive us." The CAS site was not accessible late Thursday.

Both WADA and CAS have been in the headlines recently over their handling of doping cases ahead of the Olympics, particularly regarding bans for Russian athletes following the country's doping scandals

2 Hackers Win Over 1 Million Air Miles each for Reporting Bugs in United Airlines

Source: http://www.cybersecurity-review.com/2-hackers-win-over-1-million-air-miles-each-for-reporting-bugs-in-united-airlines

Aug 09 – Two computer hackers have earned more than 1 Million frequent-flyer miles each from United Airlines for finding and reporting multiple security vulnerabilities in the Airline's website.

Olivier Beg, a 19-year-old security researcher from the Netherlands, has earned 1 Million air miles from United Airlines for finding around 20 security vulnerabilities in the software systems of the airline.

Last year, Chicago-based 'United Airlines' launched a bug bounty program to invite security researchers and bug hunters for finding and reporting security holes in its websites, software, apps and web portals.

Under its bounty program, United Airlines offers a top reward of 1 Million flyer miles for reporting Remote Code Execution (RCE) flaws; 250,000 miles for medium-severity vulnerabilities, and 50,000 flyer miles for low-severity bugs.

According to Netherlands Broadcasting Foundation, the 19-year-old reported 20 security issues to United Airlines and the most severe flaw earned the teenager 250,000 air miles.

Beg did not reveal the details about the flaws he discovered, but the teenager claims to have reported flaws in software from popular tech companies including Yahoo, Google, and Facebook.

Another 23-years-old security researcher from Algeria reported three security issues under the airline's bug bounty program and earned 1.7 Million flyer miles from the United Airlines.

iPhone bug allows hackers to steal passwords with just a text message

Source: http://www.cybersecurity-review.com/iphone-bug-allows-hackers-to-steal-passwords-with-just-a-text-message

July 01 – **Apple has fixed a major security hole that potentially allowed hackers to gain access to a user's iPhone, potentially allowing them to steal sensitive data such as passwords.**

The flaw allowed hackers to break into an iPhone simply by sending them a text message with a specially-modified image file.

When the phone's software tries to process the image, the file would exploit the vulnerability to access parts of the device's code usually off-limits to third parties such as downloadable apps. It could then execute malicious code within applications without the receiver suspecting a thing.

Security experts warned that by the iPhone trying to process the image, such as receiving a message or visiting a webpage with the picture, hackers could corrupt the iPhone's memory and access information such as website and email passwords.

The vulnerability lies in how Apple's software handles a certain image file called a TIFF. While it can render the image as normal – meaning a user will notice no difference – by tampering with an image file a hacker could also overload the iPhone's memory allowing the image to execute malicious code.

The rise of cyber insurance in New Zealand

Source: http://www.stuff.co.nz/business/industries/82774270/the-rise-of-cyber-insurance-in-new-zealand

Aug 07 – New Zealand suffers more than 100 ransomware attacks a day, according to research from Symantec.

As incidences of cyber crime increase, cyber liability insurance policies are becoming more popular in New Zealand.

But a leading cyber security expert warns organisations against jumping straight into buying cyber insurance.

BDO national leader for cyber security Leon Fouche says because of the lack of reliable data about trends, insurance companies are limited in their ability to develop robust risk modelling for the costs of cyber-attacks, resulting in restrictive terms and exclusions in policies.

A number of considerations need to be taken into account, including the level of exposure to risk, what records are at risk (personal records, for example, are at a greater risk as they are more valuable on the black market), the nature of the business and the types of cyber attacks possible.

"It's more important to look at what's not in the policy, than what is. It's like any contract. You're only going to get paid for what's in the contract," Fouche says.

Before choosing an insurance policy, organisations should do a comprehensive risk assessment, quantify those risks and then model the potential impact.

They should figure out who in the company is responsible for managing those risks, understand how effective current security systems are and work out what the appetite is to either pay an insurance premium, or accept the risk, Fouche says.

If a policy is selected, it is important for businesses to reassess their cyber risk regularly to make the policy stacks up.

BDO has recognised the changing cyber security landscape and lack of data and is conducting a new industry cyber security survey.

The survey aims to identify current cyber security trends, issues and

threats facing businesses in Australia and New Zealand.

Delta Insurance started offering cyber liability insurance in New Zealand more than two years ago and general manager Craig Kirk says New Zealand is several years behind other parts of the world.

Cyber insurance has been around internationally for about 15 to 20 years and is particularly sophisticated in the United States.

Kirk does not think the level of protection available right now in New Zealand is sophisticated enough, especially as no business is really immune from cyber crime these days.

"New Zealand, in some ways, is more vulnerable than other countries. We're seen as a soft target. The Kiwi mentality's kind of, 'She'll be right' and 'Why would anyone be interested in what I've got, this is New Zealand'."

But, he says it won't be long before most companies invest in cyber insurance.

"I think in five years' time, the vast majority of businesses will buy cyber liability insurance. The reason for that is almost every business uses the internet to trade, whether that's simple emails or having enterprise and systems online."

In Delta's portfolio, 90 per cent of cyber liability claims are related to ransomware.

An internet security threat report from internet security products company Symantec showed New Zealand had the second-highest number of ransomware attacks in the southern hemisphere.

The report showed more than 100 ransomware attacks happened in New Zealand a day, which is a 160 per cent increase from 2014.

Kirk says the largest New Zealand breach he is aware of involved an ecommerce website and cost the company about $4 million.

Rene Swindley is a director for online business insurance provider Frankie and says not enough Kiwi businesses are taking cyber crime seriously.

Frankie has experienced more customer enquiries in the last three months than ever, but overall cyber insurance uptake is slow.

Swindley says eventually, cyber insurance will be a staple form of insurance, but nothing beats preventative measures, which can be as basic as getting staff to use proper passwords that are harder to crack.

"[Proactive IT risk management] is better than any cyber insurance. Insurance goes hand in hand with that really nicely [but] if there's a company that's too relaxed about its approach to cyber security, we wouldn't be providing cyber insurance for them."

Even Solar Panels Can Be Hacked

Source: https://www.hackread.com/even-solar-panels-can-be-hacked/

Aug 09 – Do you know how you can verify if your home or property is fully secure? Well, in Fred Bret-Mounet's opinion (photo – presenting in DefCon), the only way is to try to violate the security measures yourself. And he did just that to prove his point.

Solar arrays are provided by Tigo Energy. It is a device that lets users control or monitor panels via the internet. Like every other house in California, Bret-Mounet also installed a solar array on his home but he was immensely concerned about the level of security that it provided to his family. So, he decided to check it. To his surprise, there were certain vulnerabilities in the system, with which he could easily spy on the home and even hack the power supply of a thousand homes at least. This was possible due to the open Wi-Fi access point that was linked with the MMU (Management Unit) of the solar array.

The fact that the device utilizes an open Wi-Fi access point is quite disturbing because if someone can get the login password of web account from where the solar panels could be monitored then it becomes an easy job to spy on homes.

But this was just the beginning!

In October last year, he discovered some rather serious issues. He identified that his Tigo was being served via an unencrypted HTTP connection, which was secured with an extremely easy-to-guess username and password namely "admin" and "support." To him, it was kind of a default login and he could easily manipulate the solar arrays of other residents with the same login information.

But he didn't attempt to damage his solar array but instead searched on Shodan for other vulnerable arrays on the internet and was successful in finding other Tigo systems. He then prepared to act like a malicious attacker and using the login credentials he looked for other weaknesses of the system and gained root-level access to the controller of his solar panel. This meant that he could do just about anything to his panels.

Then he identified that all Tigo devices have the same VPN connection.

"If I'd gone through that tunnel I would have reached any of them. I could have shut down a small-to-medium electricity generation facility in the aggregate, but my personal belief is that I could have used those as Trojan horses to attack targets that happened to have that type of solar panel," Bret-Mounet told Forbes.

When he contacted Tigo, the company responded quickly and the issues were supposedly being resolved in December last year. But then he was informed that the company had sold around 1000 development devices to buyers, one of whom was Bret-Mounet. Bret-Mounet also verified the company's claim by checking for vulnerable devices across the city and couldn't find any new ones. He was then delivered a production model by Tigo. But this poses an important question—how many of such devices are out there that are vulnerable to spying and hacking?

Hacker demonstrates how voting machines can be compromised

Source: http://www.cbsnews.com/news/rigged-presidential-elections-hackers-demonstrate-voting-threat-old-machines/

Aug 10 – **Concerns are growing over the possibility of a rigged presidential election. Experts believe a cyberattack this year could be a reality, especially following last month's hack of Democratic National Committee emails.**

The ranking member of the Senate Homeland Security Committee sent a letter Monday to the Department of Homeland Security, saying in part: "Election security is critical, and a cyberattack by foreign actors on our elections

systems could compromise the integrity of our voting process."

Roughly 70 percent of states in the U.S. use some form of electronic voting. Hackers told CBS News that problems with electronic voting machines have been around for years. The machines and the software are old and antiquated. But now with millions heading to the polls in three months, security experts are sounding the alarm, reports CBS News correspondent Mireya Villarreal.

For weeks, Republican presidential nominee Donald Trump has told his supporters the outcome of the 2016 election could be out of his control.

"I'm afraid the election is going to be rigged, I have got to be honest," Trump said to Ohio voters last week.

But for the hackers at Symantec Security Response, Election Day results could be manipulated by an affordable device you can find online.

"I can insert it, and then it resets the card, and now I'm able to vote again," said Brian Varner, a principle researcher at Symantec, demonstrating the device.

The voter doesn't even need to leave the booth to hack the machine.

"For $15 and in-depth knowledge of the card, you could hack the vote," Varner said.

Symantec Security Response director Kevin Haley said elections can also be hacked by breaking into the machines after the votes are collected.

"The results go from that machine into a piece of electronics that takes it to the central counting place," Haley said. "That data is not encrypted and that's vulnerable for manipulation."

"How big of a hacking potential problem is this?" Villarreal asked him.

"Well, there's a huge potential," Haley responded. "There are so many places in the voting process once it goes electronic that's vulnerable."

According to a report from the Brennan Center for Justice, one reason these voting systems are so vulnerable is their age.

"We found that more than 40 states are using voting machines there that are at least 10 years" old, Brennan Center for Justice researcher Christopher Famighetti said.

Denise Merrill, president of the National Association of Secretaries of State, said the lack of funding keeps most precincts from updating their systems. But all machines have to meet specific government standards.

"The idea of a national hack of some sort is almost ridiculous because there is no national system," Merrill said.

In fact, the more than 9,000 voting districts across the country all have different ways of running their elections -- down to the type of machine they use. But Merrill said there are checks in place to prevent fraud.

"Our voting systems are heavily regulated. They're tested both before and after. There are paper trails everywhere...by in large, I would say the American election system works very well," Merrill said.

CBS News learned that only 60 percent of states routinely conduct audits post-election by checking paper trails. But not all states even have paper records, like in some parts of swing states Virginia and Pennsylvania, which experts say could be devastating.

The Election Assistance Commission told CBS News that it ensures all voting systems are vigorously tested against security standards and that systems certified by the EAC are not connected to the Internet.

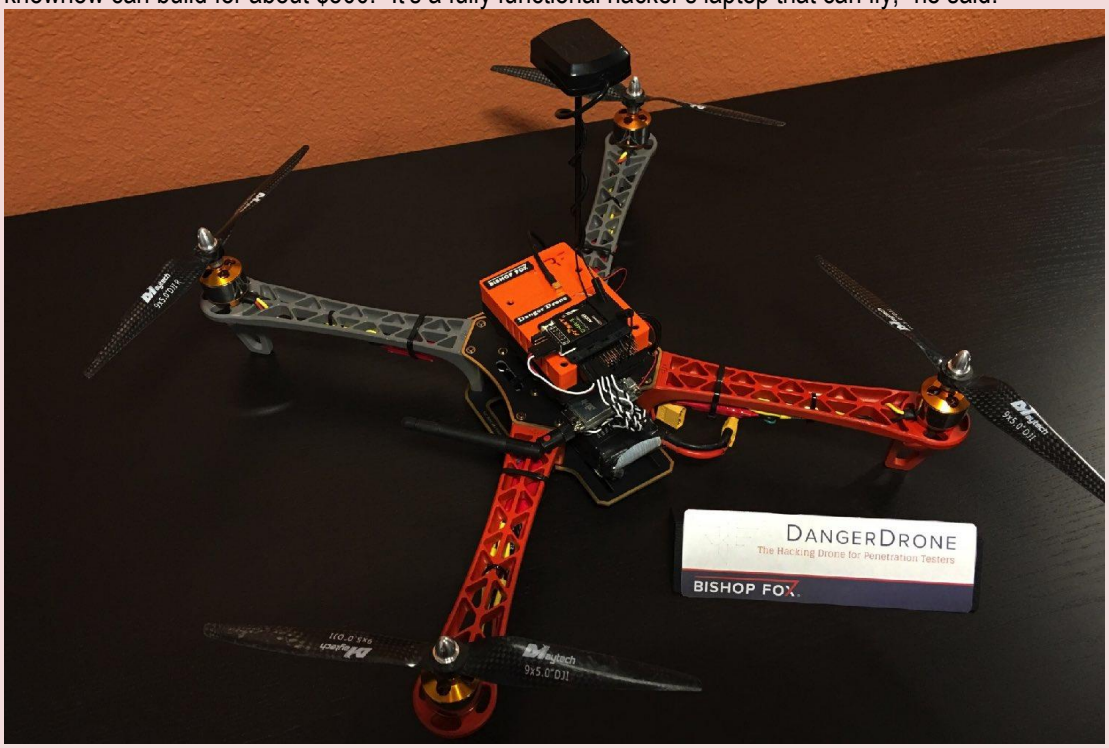
Credit Card Size Drone to Test Networks

Source: http://i-hls.com/2016/08/credit-card-size-drone-to-test-networks/

Aug 12 – At the recent Black Hat hacker conference in Las Vegas, cybersecurity researchers showed how drones can help secure wireless networks and bulster cybersecurity.

David Latimer, an analyst at the cybersecurity firm Bishop Fox, demonstrated the Danger Drone, a custom-built quadcopter drone the size of a credit card that anyone with enough technical

knowhow can build for about $500. "It's a fully functional hacker's laptop that can fly," he said.



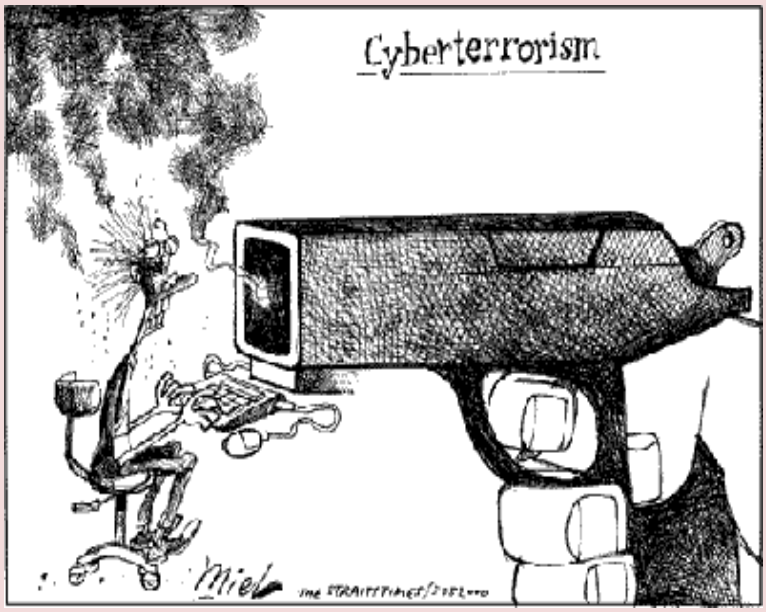
According to Digital Trends, the goal was to make a cheap, easy-to-create hacking drone so that cybersecurity professionals can test out the defenses that they're rolling out. It's a drone for penetration testing, to see how effective the defenses against this kind of thing actually are.

According to the Christian Science Monitor, the idea behind Danger Drone is that professionals would deploy it to remotely test the resiliency of Wi-Fi or Bluetooth networks outside office buildings, attempt to penetrate the networks using the drone, and then patch the vulnerabilities.

Melrose says increasingly small and powerful drones could inflict significant damage if in the wrong hands.

The rise of a cyberterror community is on the horizon

Source: http://www.homelandsecuritynewswire.com/dr20160816-the-rise-of-a-cyberterror-community-is-on-the-horizon



Aug 16 – According to Max Kilger, director of Data Analytics Programs at the University of Texas at San Antonio (UTSA) College of Business, the rise of a cyber terror community is on the horizon. Kilger, who utilizes his talents as a social psychologist as well as a cybersecurity expert, believes that this new community may be the logical next step in the development of our digital world.

"I've been studying the digital community

for a long time and framing the events there in terms of social movement theories," he said. "I've been able to classify their social stories into distinct epochs. The first epoch saw the rise of the hacking community."

USTA says that Kilger, also a faculty member of the UTSA Department of Information Systems and Cyber Security, pointedly distinguishes the hacking community from the cybercrime community. He says the cybercrime community likely evolved as a social movement "spinoff" from certain elements within the hacking community as their skills became financially lucrative to criminals thus forming the second epoch in the digital world.

"Anthropologists have studied this kind of phenomenon in indigenous cultures that have never been exposed to money. It sometimes just wreaks havoc. They change dramatically or even end up destroying themselves," he said. "I think that is what is responsible for the start of the cybercrime epoch."

The injection of money into the hacking community led outsiders like organized crime members to suddenly have significant power in a group that once operated as a meritocracy based solely upon technical expertise.

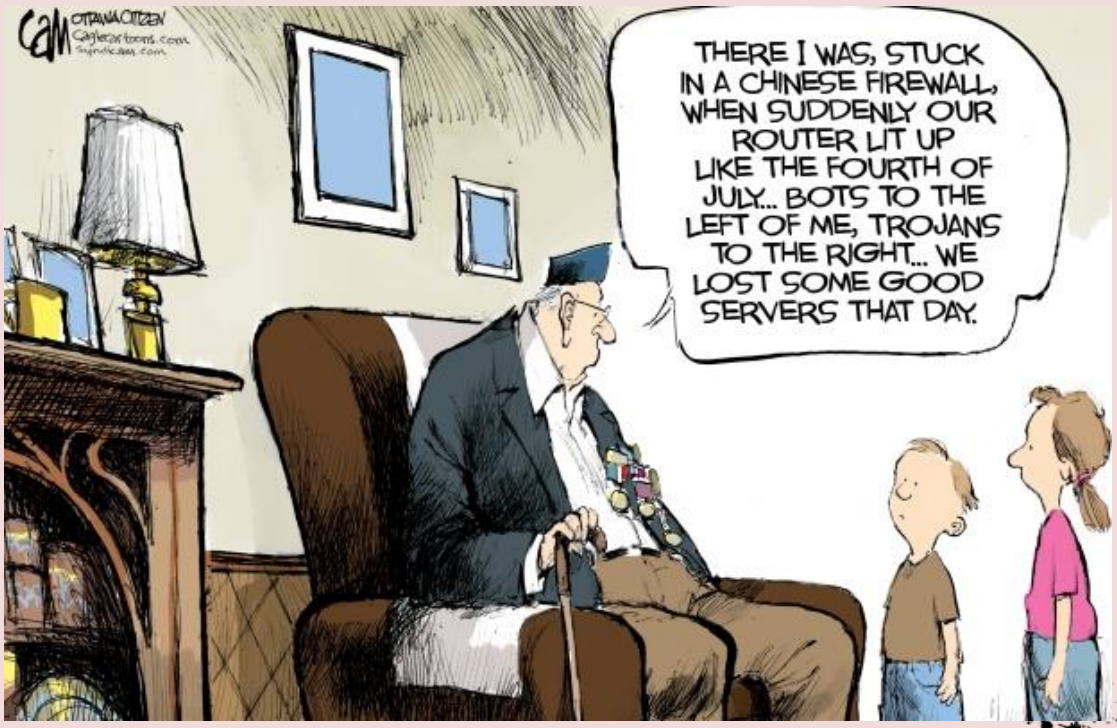
"The cybercrime epoch is still forming and growing," Kilger said. "It's becoming more organized and gaining more social structure. Cybercriminals now even have customer service and money-back guarantees on stolen financial assets such as credit cards or banking credentials."

Kilger recently represented UTSA at a NATO training facility in Ankara, Turkey where he presented his theory about the potential third epoch of our digital world: the possible emergence of a cyber terror community.

"The magnitude of potential damage for a cyberattack is remarkable, and the number of targets for a cyber terrorist attack is amazingly large," he said. "The chance of getting caught are very small, and some of the resources to complete the crime are very easy to obtain — not to mention the potential for getting away with it is very high."

According to Kilger, the idea that terrorists are only motivated by geopolitical, religious, or ethnic causes may be outdated in our digital world. Other motivations for malicious online acts such as money, ego, entrance to social group, or status may emerge as motivations for cyber terrorists as well. He stresses the need to think beyond these traditional motivations as cyber terror becomes more prevalent.

"If we look at the history of the digital age and look forward with a theoretical approach, there's a much greater chance that we can understand and predict future cyber terror events," he said. "That's an important milestone in and of itself."



6 Rules for Social Media Use Before and During a Crisis

By David Kalson

Source: http://www.preparedex.com/6-rules-for-social-media-use-before-during-a-crisis/

Aug 01 – As is painfully well known to many companies that have endured crises, social media can be a troublemaker: An irate consumer posts a recording she captured of some impolite customer service she experienced from your company, and it's being re-Tweeted *ad nauseum*. Or, a diner's video of a cockroach backstroking through your restaurant's clam chowder goes viral on YouTube and Facebook. The upshot is you've got a serious threat to your company's reputation on your hands being driven by social media, and it very well could grow into a full-blown crisis.

But many companies also know that social media can be a potent tool for solving the problem. Here are six rules for leveraging social media before and during a crisis:

Before a crisis: Prepare

1. **As part of your Crisis Plan, include the establishment of a productive presence on social media.** Embrace social media platforms to project your brand attributes. Convey confidence in your products. Show pride in your good corporate citizenship actions, environmental policies, and so on. All of these things work to establish your organization as one of living, breathing humans who care about their customers, communities and planet. Your organization's humanity and projection of it through social media channels is a necessary prerequisite for effective communications when a crisis hits.
2. **Create a social media policy for your employees.** Do you want your employees to talk about your company as they hobnob with their friends and family on Facebook, or post photos of their workspace on Pinterest? Whether you do or you don't, employees must understand their obligation to protect the source of their livelihoods. They must be given clear guidelines as to what is expected of them in their social media use.

If no policy exists and a crisis occurs, employees' social media conduct could make matters worse. *"Yeah, sometimes our customer service really does suck." "I work back in the kitchen, and I've seen those cockroaches doing water ballet in the chowder."* Clearly such employee postings during the crisis will worsen the problem, and it will be far more awkward for management to suddenly impose rules for social media. You need to have a social media policy for employees in place now. It's a cornerstone of crisis preparedness.

3. **Monitor and assess.** Whether they're good, bad or ugly, it's important to keep abreast of social media conversations involving your organization and continuously gauge the volume and consistency of positive and negative comments. You can then decide when a tipping point has been reached, indicating a crisis might be brewing and preemptive actions need to be taken.

4. **Address the crisis.** If you've successfully established your social media presence as part of your crisis preparedness, you have a platform people know to go to for information. If you were to try to establish a social media presence after the crisis is already underway, it would likely come off as a suspiciously defensive measure that could do your organization more harm than good.

Your ongoing social media presence serves as a positive framework that surrounds and gives perspective to any particular sub-set of crisis-related messages you need to convey. *"We are truly sorry for the bad customer service you received (or egregious dining experience you recently had) and have investigated the matter. What we found was a serious violation of the policies we have in place, and we have taken the following actions to make things right:…; we will gladly provide a refund…; etc., etc."* The crisis is addressed and then you move back to announcing your new sale items or your educational program for disadvantaged kids. An ongoing social media presence isolates particular crisis-related messages, containing them within a wider, more reasonable, more human context.

5. **Engage – Selectively.** You will of course be closely monitoring social media (and all other media) during a potential or actual crisis; it's an important indicator of the effectiveness of your crisis management. You then use your constant evaluation of that information to help inform your ongoing communications strategies.

Probably you will not want to respond to every negative posting. But, you might decide to engage. It's a strategic decision you'll have to make depending on the substance and number of complaints and on the influence of individual complainers.

6. **Determine how or if to coordinate your social media engagement with your website content.** Some social media-driven crises may be best handled exclusively through social media. This is often the considered strategy when there are customer complaints appearing with some regularity on social media sites, but they haven't yet reached what the company determines to be a critical volume. In this case, companies will not post their crisis-related responses on their website believing it will draw even more interest to the situation unnecessarily and further feed social media exchanges.

If the volume of interest on social media has reached that tipping point where your business and reputation is continuously threatened, you may decide to coordinate your social media engagement with crisis messages on your website.

Sometimes companies purposely bury the crisis-related material on their sites so you'd have to search hard for it – a sort of middle ground, but not necessarily advisable. Try to find, for example, VW's messages about its emissions cheating scandal on its website. They're there, but you have to search hard to find them. This obfuscation strategy, while often very carefully considered and quite common, carries a risk. It could contradict pledges many companies make to be transparent and worthy of your trust.

For the most dire crises, messages that you deliver in social media conversations should usually be coordinated closely with easy-to-find messages on your website. That often entails creating new web content in its own dedicated section during the crisis. Some companies maintain a so-called "dark site" that's nearly ready to go and can be finalized and made to go live quickly in a very serious crisis.

After the crisis

If you've been successful in managing the crisis, it's now been consigned to past history and you've moved on. But not so fast. Now is the time to carefully analyze what happened and the effectiveness of your response. Use the experience to improve your crisis preparedness in general and your social media policies, monitoring and engagement strategies in particular.

Modify your crisis plans accordingly and test that plan through regular simulated crisis exercises that should always include a social media component. Only then will you be as prepared as you possibly can be to respond to thousands of amused people who have been sharing a clever video of a cockroach water ballet in your restaurant's soup.

David Kalson *is an expert in issues and crisis management. He has more than 25 years experience providing strategic communications counsel, on-the-ground assistance and highly targeted media relations and "new media" programs to manage issues and crises as well as reputation enhancement for both profit and not-for-profit organizations. Business sectors he has counseled include energy,*

food and beverage, financial services, healthcare, consumer products and technology. He has designed and implemented communication / media relations programs, often emphasizing Web-based strategies, to address issues including data security breaches, environmental accidents, product recalls, financial problems, high-profile lawsuits, corporate governance issues, criminal behavior, attacks by opposition groups, government/regulatory challenges, competitive challenges and labor disputes. Companies he has counseled in relation to crisis drills, plans and crisis management include Cargill, Dunkin' Brands, Cadbury Schweppes, Staples, Entergy, Eli Lilly, Canaport LNG and the American Automobile Association (AAA).

Ambushed!

By Erik Bernstein

Source:http://www.preparedex.com/ambushed/?mc_cid=173f9f85c7&mc_eid=5237985c4f

When you run into crisis you expect to encounter the media, but where I often see even the well-coached run into trouble is when they're caught by surprise. A news crew showing up at your offices likely has to make their way through several layers of interference before you're actually in front of them, but a news crew rolling up to your driveway as you get home from work or jumping out as you head to your kid's soccer game on Sunday morning is a very different situation. The combination of not being in "work mode", tiredness, and utter surprise has led many to dig a nice big hole for themselves to jump into.

So, what are your options when the media catches you unprepared? Luckily, you have a few.

1. The gracious delay – One of the easiest and most effective ways to fend off ambush interviews is by putting on your most gracious attitude and simply telling the reporter, "I would love to share more with you on that, will you please send your questions via email so that I can give you a full response?" Even if there's a camera in your face you come off as reasonable and willing to answer, while avoiding saying anything until you've had time to catch your breath and think.

2. Defer to the correct authority – Often, questions are thrown that are not your responsibility to answer. Don't speculate when there is an authority on that issue, instead show how helpful you are by informing the reporter of where they can seek the proper information. A common example of this is when local law enforcement is involved; while you may be able to speak to what caused someone to be arrested, you are not the person to provide any detail as to what law enforcement is doing as a result.

3. Cite lack of information – If you're facing a question you should answer, but simply don't have the information to answer it properly, it's actually okay to say so. Telling a reporter that you don't know the answer yet, but that you will share your findings as soon as you can, is a legitimate way to avoid losing face. Be careful with your promises however. Especially in cases where there is pending litigation you may not be able to share what you said you would.

Gone are the days of throwing "no comment" left and right as you briskly walk away. Today's media climate means a response is required, and if you don't give it to them it's as good as shouting, "we're guilty!". Don't neglect the fact that who can be a reporter has expanded immensely as well, and someone with a cell phone and a list of pointed questions can do just as much damage as the truckload of folks sent over by Channel 5.

Know the possibilities and prepare for them, or you're putting your organization at risk.

Erik Bernstein *is a seasoned social media manager and crisis management consultant. Brought up in the trenches as part of the Bernstein Crisis Management team, he prides himself on his understanding of how to best handle conversation and reputation management strategy across all forms of communications. Of course it's not all work, and when not conducting serious business he loves to read, prepare all*

types of food, from fried Twinkies to beef Wellington, and pretend he's a pool shark on his favorite ratty old table.

Fire guts Emirates jet after hard landing; one firefighter dies

Source: http://www.reuters.com/article/us-emirates-airplane-crash-idUSKCN10E0Z7

Aug 03 - An Emirates jetliner arriving from India caught fire after slumping onto the runway in Dubai on Wednesday, killing one firefighter in an intense blaze and bringing the world's busiest international airport to a halt for several hours.

All 300 passengers and crew were safely evacuated from the gutted Boeing 777-300 after a crash that one survivor described as terrifying. Fourteen people were admitted to hospital.

The Dubai carrier's first significant accident happened after the crew apparently attempted to abort the landing for a second attempt amid unconfirmed witness reports of landing gear problems.

Video showed a tower of flame bursting from the front of the plane, and then a thick black plume of smoke rising into the sky. Reuters was unable to verify the footage independently.

Photographs on social media showed a plane lying crumpled on the tarmac with black smoke pouring from its upper section, and later images showed a gap along the length of the charred fuselage where its roof had been.

"It was actually really terrifying. As we were landing there was smoke coming out in the cabin," said passenger Sharon Maryam Sharji. "People were screaming and we had a very hard landing. We left by going down the emergency slides and as we were leaving on the runway we could see the whole plane catch fire. It was horrifying."

Another passenger leaving the airport with his family said there had been a problem with the landing gear.

A spokesman for operator Dubai Airports said everyone aboard flight EK521 coming from Thiruvananthapuram in southern India had been evacuated.

Go around attempt

Flights at Dubai International resumed at 6:30 p.m (1430 GMT) after all arrivals and departures were suspended for over five hours, authorities said.

According to air traffic control recordings cited by Aviation Herald, a respected independent website monitoring air accidents, controllers at Dubai reminded the crew of the Boeing 777 to lower the landing gear as it came into approach.

Shortly afterwards, the crew announced they were aborting the landing to "go around," a routine procedure for which pilots are well trained. But the aircraft came to rest near the end of the runway instead, Aviation Herald reported.

It was not immediately clear whether the landing gear was extended by the time the aircraft touched the ground at around 0845 GMT, though a family of passengers who declined to be named said the wheels did not deploy and the jet landed on its belly.

Unverified amateur video posted on Twitter appeared to show the plane sliding on its belly moments after landing, with its right engine torn away from its usual position under the wing.

Emirates initially said there were 275 passengers and crew aboard the plane, in service with the airline since 2003, but later updated that number to 282 passengers and 18 crew.

Both the airline and aircraft have a solid safety record. It is the first time an aircraft operated by Emirates has been damaged beyond repair since the carrier was founded in the 1980s.

The crash is nonetheless a blow to the Dubai carrier weeks after it was voted the world's top airline by Skytrax at the Farnborough Airshow, taking the crown from rival Qatar Airways.

Emirates carried 51.3 million passengers in 2015 and is the world's fourth largest carrier in terms of passenger traffic. It has over 250 aircraft, including the world's largest fleet of Airbus A380 and Boeing 777 jets.

Firefighter killed in action

Airline chairman Sheikh Ahmed bin Saeed al-Maktoum said a Dubai firefighter died while trying to put out the flames.

Jassim Essa Al-Baloushi, was the firefighter killed while tackling the blaze.

He said the plane had undergone maintenance in 2015 and that the United Arab Emirates pilot had over 7,000 hours of flying experience.

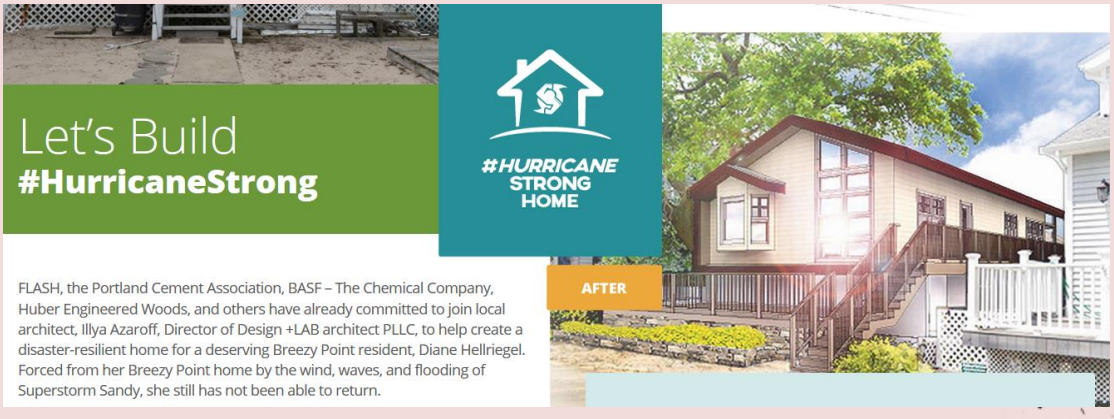
Safety experts said it was too early to pinpoint a cause for the crash, but Sheikh Ahmed ruled out any security breach.
Boeing (BA.N) said it would work with Emirates to gather more information.
Investigators will scour the wreckage and interview pilots, controllers and witnesses for clues to any technical malfunctions, human error or weather-related problems.
Judging by footage of the aircraft's intact tail section, where the 'black box' flight recorders are located, vital voice and data recordings should be retrievable.
According to specialist aviation weather reports, at the time of the accident temperatures at Dubai International airport were up to 49 degrees Celsius (120 degrees Fahrenheit) and wind shear - a potentially hazardous condition involving sudden and unpredictable changes in wind direction or speed - was indicated on the airport's runways.

Build disaster-proof homes before storms strike, not afterward

By T. Reed Miller

Source: http://www.homelandsecuritynewswire.com/dr20160808-build-disasterproof-homes-before-storms-strike-not-afterward

Aug 08 – On Breezy Point in Queens, New York, construction will start soon on Diane Hellreigel's new house. Dubbed the #HurricaneStrong Home, it will replace a house built in 1955 by Hellriegel's grandfather that was wrecked during Superstorm Sandy in the fall of 2012.
The demonstration home was designed by private companies working with the Federal Alliance for Safe Homes, or FLASH, a nonprofit coalition that promotes action to strengthen homes and prepare for disasters. It features a solid concrete foundation that elevates the living space above floods, and uses



energy-efficient insulated concrete form (ICF) for the walls and floors designed to withstand wind and blown debris.

The roof deck of the demonstration home uses principles from the Fortified Home standards, a set of national guidelines designed to improve on minimum building codes and make structures more disaster-proof. They include taped plywood seams to prevent water entry, and reinforcing spray foam insulation underneath the roof to help keep wind from blowing it off and also improve energy efficiency.
Projects like the #HurricaneStrong Home demonstrate that there are many technologies we can use to make our buildings more hazard-resistant. But we are not using them as extensively as we should. Instead of designing a building to reduce potential damage from the hazards it may face over its lifetime, most construction projects focus on saving money up front. By choosing the lowest construction cost possible, homeowners, insurance agencies, and taxpayers may end up paying for it many times over when natural disasters occur.

Forecasting storms and mitigating damage

Although we cannot always predict far in advance when a disaster will strike, we do know that climate change will result in more frequent and intense storms than in the past. Hazard modeling has progressed considerably over the past several decades, and we can make strong predictions of roughly how often to expect disasters from coast to coast.

The Monolithic Dome

Researchers from a variety of disciplines are developing tools that can help us make smarter decisions about mitigating storm damage by preparing the built environment in advance. FEMA has designed free software tools that embed hazard models to help evaluate the impacts of disasters on individual buildings and the larger community. The Benefit Cost Toolkit compares the effectiveness of different mitigation strategies for a particular building and location. The Hazus-MH software maps out expected damage in a community from multiple hazards and allows comparison of "what-if" scenarios, such as "what would the economic benefit be if this community reinforced or rebuilt its vulnerable building stock?"
At the MIT Concrete Sustainability Hub, we are creating life cycle cost analysis models to include the costs and benefits of mitigation efforts alongside operational costs such as utility bills and maintenance. In our case studies we have demonstrated that investing in more hazard-resistant residential construction in certain locations is very cost-effective.
We have also developed a metric called the Break Even Mitigation Percent (BEMP) to address the cost-effectiveness of mitigation features for a particular new building in a particular location. The BEMP factors in the expected damage a building designed to code would endure over its lifetime, compared to a more resilient building design.
As an example, we compared two designs for a four-story apartment building located on the Gulf or Atlantic coasts – one constructed with nonengineered wood, the other with more resilient engineered concrete – and modeled the damage that these buildings would be expected to sustain over fifty years. For a building sited in Galveston, Texas, we estimated a BEMP of 3.4 percent, meaning that if $340,000 was invested on top of the initial $10 million costs in order to build the stronger version, that investment would mitigate enough storm damage to the building over its lifetime to pay for itself.
It is important to note that BEMP considers costs from the perspective of society at large. That's because the original homeowners might not occupy a building thirty years later when a hurricane rolls through, so they might not directly recoup the value of investing in a resilient design – unless the mitigation features allow them to resell the house at a higher

value, which can happen. But insurance agencies, taxpayers and future occupants certainly will all benefit from investing up front to make buildings more storm-resistant. Neighboring homes will also benefit from fewer building material projectiles flying off storm-resistant homes.

Injecting mitigation into building codes

More hazard-resistant buildings produce broad social benefits. If a community can recover from a disaster more quickly, the disaster's negative impact on the economy and vital systems like health care and education can be reduced. Importantly, hazard resilience means lives can be saved.

But architects and designers often have a different incentive: keeping construction costs low. This is why most new construction projects just meet code requirements, instead of making extra investments to weather disasters well. Builders do not often consider reconstruction costs – the money that owners, insurance agencies and taxpayers will spend in the future to recover after the first structure fails in a storm.

To address this disconnect, the nonprofit International Code Council spearheads Building Safety Month each May to spotlight the need for modern building codes, more aggressive code enforcement and better training for building inspectors. However, the United States does not have a national building code with federal enforcement. Instead states, and sometimes municipalities, devise their own approaches. This patchwork system is inefficient and ineffective. A similar situation exists in cyclone-prone Australia.

This past May the White House hosted a Conference on Resilient Building Codes to highlight the importance of developing codes that incorporate resilience and future climate change impacts. One state that has embraced this approach is Florida, which adopted progressive statewide building codes after Hurricane Andrew in 1992. These requirements have substantially reduced insured losses in subsequent hurricanes.

Congress underfunds mitigation

At the federal level, though, most spending on mitigation occurs after disasters strike. Up to 15 percent of federal assistance can be allocated to long-term hazard mitigation measures after the president declares a major disaster. For instance, after a hurricane, states often use these funds to retrofit and elevate buildings, protect infrastructure and utilities, and manage stormwater.

The Federal Emergency Management Agency (FEMA) also awards pre-disaster mitigation grants (PDM), which states and communities can use to reduce risks from future events. But recent Congressional appropriations for PDM have fallen far short of what is needed. Last year FEMA requested $400 million for PDM but received only $81 million. From 2005 to 2014, appropriations averaged just $120 million each year. Compare that to the $7.2 billion spent on average on recovery assistance; PDM grants accounted for only 1.6 percent of total FEMA grants on average.

Recognizing that the current approach is not sustainable, this spring FEMA proposed a disaster deductible. The policy would require states to invest in resilience efforts before receiving public assistance funding after a disaster.

Post-Sandy rebuilding in New York

Diane Hellreigel's home was among 100,000 damaged in New York during Superstorm Sandy. Of those, 20,000 owners applied for New York City's Build It Back program in 2013, but construction has been completed on only 1,887 units. City leaders are working to make New York more resilient against future disasters through steps that include funding coastal protection projects and modifying local building codes pertaining to flooding.

Congress earmarked over $13 billion to fund Hurricane Sandy recovery in New York City alone. That sum includes $595 million for FEMA assistance to affected individuals and families. Overall, however, just 5.3 percent of FEMA funding for Sandy went toward hazard mitigation grants.

These efforts are encouraging, but many coastal and inland communities remain vulnerable to natural disasters. To prevent the devastation from another storm, twister, or quake, we need to make deep investments nationwide in mitigation now, before the next disaster strikes.

T. Reed Miller *is Researcher in Environmental Engineering & Technology Policy, Massachusetts Institute of Technology.*

NICS, a communication platform for first responders, now available

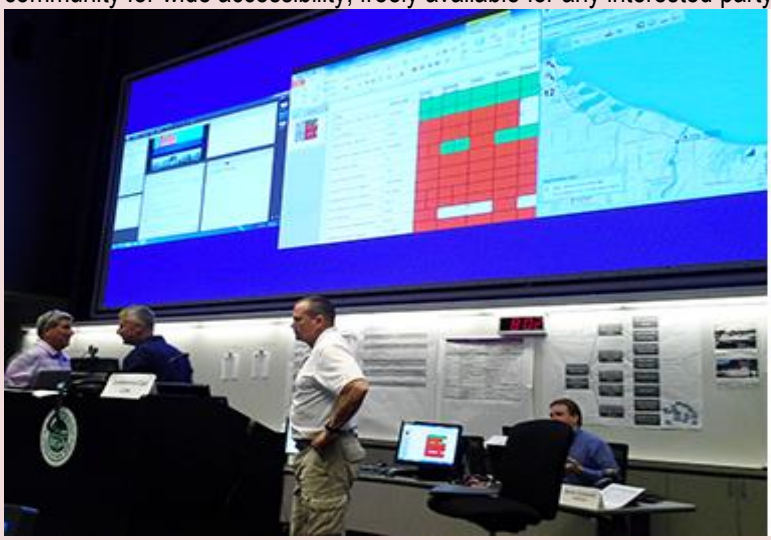
Source: http://www.homelandsecuritynewswire.com/dr20160809-nics-a-communication-platform-for-first-responders-now-available

Aug 09 – The U.S. Department of Homeland Security (DHS) Science and Technology Directorate (S&T) has announced the **Next-Generation Incident Command System (NICS,)** an information sharing tool for first responders, is now available worldwide.

NICS is a mobile, Web-based communication platform that enables responders on scene at a

developing incident to request and receive assistance from remote experts, such as a university researcher or topographic expert, in real time. Conversely, experts can observe an evolving situation and volunteer relevant material or resources.

S&T says that after successful beta-implementation, NICS has transitioned to the open-source community for wide accessibility, freely available for any interested party.



"Through strong partnerships within the State of California, responder organizations across the United States, and the State of Victoria in Australia, NICS software is deployed as an operational tool in many first responder communities," said Dan Cotter, director of S&T's First Responders Group. "And now that the platform code has been made available to the open-source community, first responders can leverage this tool from anywhere in the world."

DHS S&T has led the funding of the development of NICS with contributions from the U.S. Coast Guard Research and Development Center at the Massachusetts Institute of Technology Lincoln Laboratory (MIT-LL) since 2010.

In 2014, Emergency Management Victoria launched its information sharing environment using the NICS code while it was still in research and development. In April 2016, the California Governor's Office of Emergency Services (Cal OES) also deployed the NICS software as the Situation Awareness & Collaboration Tool (SCOUT) for California emergency responders.

The NICS vision has been further advanced with Cal OES, the California Department of Forestry and Fire Protection (CAL FIRE), and numerous local fire, law enforcement, and emergency management agencies across California and the United States.

During the September 2013 "Rim" wildland fire in Yosemite National Park, burning 235,000 acres, and numerous organizations deployed NICS to make collaborative decisions and disseminate the constantly developing information.

Because of the success of these partnerships — and the advancements they have enabled — DHS S&T successfully transitioned the NICS software from a research and development effort to an operational capability.

DHS says it will manage the core NICS open source code and is in the process of transitioning the capability through three venues:

1. NICS source code is now available to first responder and emergency management agencies and may be found on the U.S. government's open source code repository site, GitHub.
2. The Worldwide Incident Command Services Corporation, Inc., a California-based non-profit, has implemented the NICS code as RAVEN.
3. In Fall 2016, the NICS capability will be hosted within the DHS Homeland Security Information Network (HSIN) as part of the Geospatial Information Infrastructure for Homeland Security users.

"Moving forward, these domestic and international partnerships will continue collaboration on the NICS open-source code," S&T says.

Emergency crews may control traffic lights at Abu Dhabi intersections

Source: http://www.thenational.ae/uae/transport/emergency-crews-may-control-traffic-lights-at-abu-dhabi-intersections

Aug 13 – **Motorists are warned that crews of emergency vehicles may be given the power to take control of traffic lights at intersections on the capital's roads.**

The Abu Dhabi Department of Municipal Affairs and Transport is testing an emergency vehicle priority system which allows civil defence, ambulance and rescue services to send signals to lights as they approach them.

Work began in March 2014 on Abu Dhabi's new central traffic control system, using about 20 sensors at each intersection to monitor the volume of traffic.

The system can give priority to emergency vehicles and buses and respond to variations in traffic flows by reducing delays and queue lengths at junctions.

The launch date for the system is yet to be decided.

"Those are the smart traffic signals that are being implemented in Abu Dhabi and Dubai," said Phil Clarke, a principal road safety consultant at Transport Research Laboratory UAE.

In the UK, a similar system is in place to give priority to buses.

"The system enables emergency vehicles to have a freer passage

through the traffic signals and prevents a tailback of traffic and emergency service vehicles not being able to fight through the traffic to get into the intersection," Mr Clarke said.

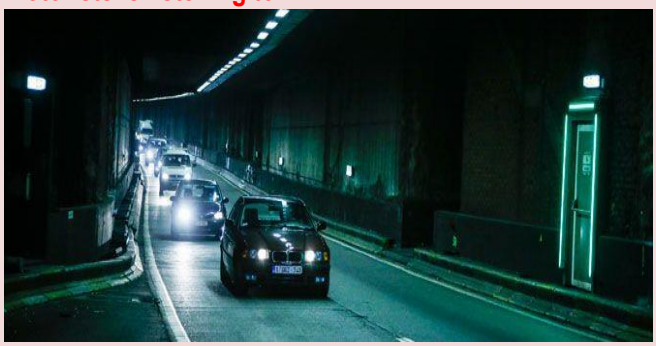
"If you're thinking about deploying your emergency services and you've got this facility, you will know more accurately what the response time would be from the

civil defence station, for instance, to certain locations."
If an ambulance can travel more quickly to a site, the system might help to resolve large congestion problems there, said Michael Dreznes, executive vice president of the International Road Federation.
"This will allow the traffic to return to normal at a much faster rate," he said. "It should also reduce the likelihood of side impact collisions, commonly called T-bone accidents, at intersections."
Experts urged motorists to pay attention to emergency vehicles as they make their way to help others.
"If you've got an ambulance behind you, or civil defence or police that is clearly on an emergency call, just try to move over and give them room to go through," Mr Clarke said.
"But if you don't see the size of an ambulance or civil defence lorry in your mirror, you're clearly not paying attention to what you're doing."
While some do give way to emergency vehicles, other drivers panic and are unable to clear the path for them, said P M Abdul Razak, assistant manager at Emirates Driving Institute's instructor training centre.
"Novice drivers may find it difficult to spot a safe gap when an emergency vehicle is approaching," he said. "While on the move, some drivers are scared to change lanes and unintentionally block the vehicle."
Not giving way could cause a serious accident or lead to an ambulance being out of action.
"All drivers must check their rear-view mirrors frequently for any emergency vehicle travelling behind them," Mr Abdul Razak said. "They should indicate their intention to pull over in a space to allow the vehicle to pass safely, and watch out for other emergency vehicles as there may be more than one."

Brussels to launch "FM break-in" system in tunnels

Source: http://deredactie.be/cm/vrtnieuws.english/Brussels/1.2733596

Aug 08 – **Before the end of the year road tunnels across Greater Brussels will be equipped with "FM break-in" technology. The FM break-in system will allow Mobile Brussels to send messages to motorists via their in-car stereo systems. The messages break into the radio programme the motorists is listening to.**



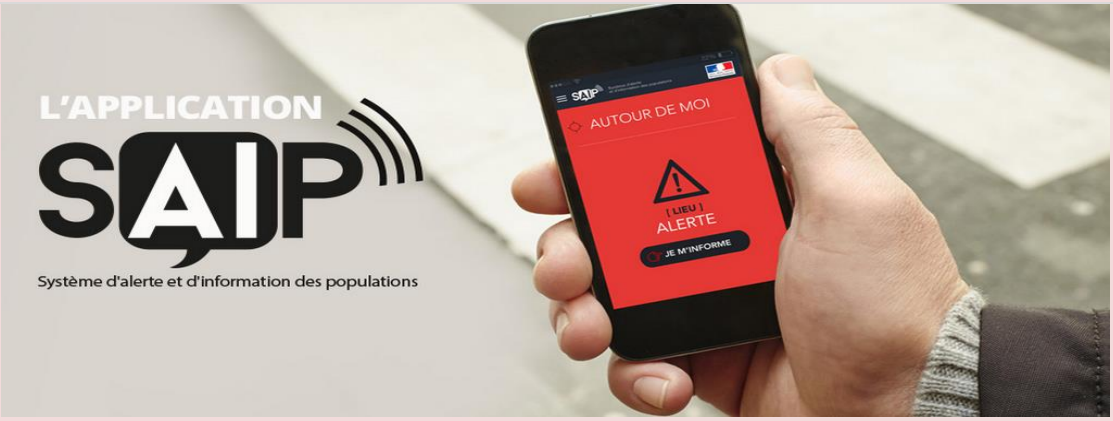
The system will only be used in case of emergencies such as fires. The messages will contain a warning and more information about the dangerous situation.

The messages will be broadcast in both Brussels' official languages: French and Dutch. The messages will only contain information about dangerous situations. Traffic and travel news will not be broadcast via the system.
Mobile Brussels will use its tunnel radio re-broadcast system to broadcast the FM break-in system. The system will of course only work if the radio is switched on.
Mobile Brussels says that the system should be up and running before the end of the year. "This is a first step towards improving the way in which we keep the public informed", Mobile Brussels' Inge Paemen told VRT News.

When disaster-response apps fail

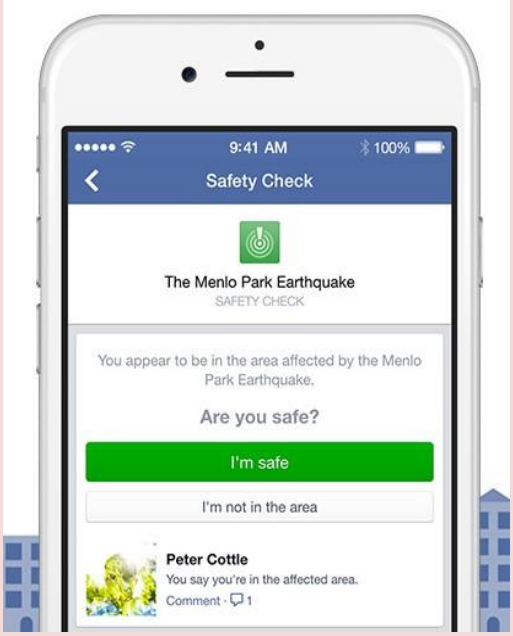
By Nicholas Kman
Source: http://www.homelandsecuritynewswire.com/dr20160812-when-disasterresponse-apps-fail

Aug 12 – When a terrorist struck Nice, France, on 14 July, a new French government app designed to alert people failed. Three hours passed before SAIP, as the app is called, warned people in and around Nice to the danger on the city's waterfront during Bastille Day festivities.



This aspect of the tragedy highlights an emerging element of disaster preparation and response: the potential for smartphone apps, social media sites, and information technology more broadly to assist both emergency responders and the public at large in figuring out what is happening and what to do about it.

A group I am in, with researchers from varied disaster-response backgrounds (including military, urban, wilderness and hospital service), has surveyed what's already available on the market and found smartphone apps that can help providers and the public alike. Some help medical professionals deal with ordinary day-to-day work, viewing guidelines and medication databases, performing calculations, remotely monitoring patients' vital signs and



displaying radiology images. Others can help responders deal with chemical, biological, radioactive, nuclear and explosive disasters, which is useful for members of FEMA teams like the one I'm on. Apps for the public help them prepare for disasters, notify them of imminent problems, reconnect them with family members, and even help keep track of pets during emergencies.

But as the failure of the French app during the Nice attack illustrates, communication is almost always a problem during disasters – no matter what kind of problem it is: weather-related, an attack of some kind or even just a power outage. Effective communication, such as an evacuation alert as a hurricane approaches, can save lives. Unfortunately, as we saw during Hurricane Katrina, disasters can themselves cause damage resulting in communications breakdowns. This problem is best solved by emergency planners using the same strategy individuals figured out for themselves in Nice: create multiple independent systems to ensure connectivity.

Planning for redundancy

In disasters, many emergency responders already anticipate communication failure and employ multiple systems. Hospitals, for example, handle most communication with paging systems and in-building intercoms. If those go down, doctors, nurses and other staff can reach each other on their cellular phones. Should those fail, many hospitals keep closets full of radios charged and ready for use.

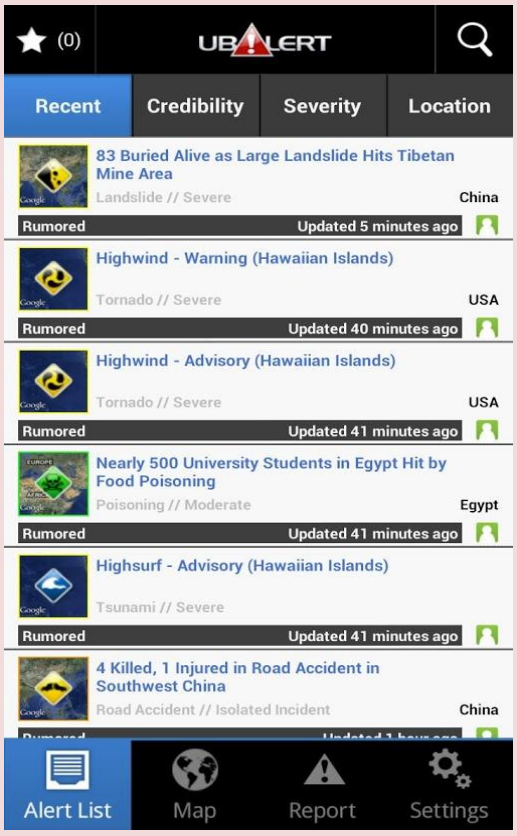
This principle holds true for social media and smartphone apps, too. The SAIP app's failure was due in part to its developer's lack of attention to redundancy, according to French news reports, as well as an accidentally severed fiber-optic cable and a software error.

Although the SAIP app failed, citizens were able to communicate via social media. Citizens of Nice took to Facebook to use its Safety Check feature to post that they were safe, and to make sure friends

and family had checked in OK. This type of organic social media communication also happened after the Boston Marathon bombing: People near the explosions quickly posted Twitter messages identifying the location and specifics of events, as well as their own whereabouts and safety.

Most of the newest technologies in communication and disaster response employ this crowdsourcing technique. The FEMA app allows users to upload pictures and information about disasters, in addition to sending out information from the National Weather Service and other government agencies.

The ubAlert — Disaster Alert Network App



works similarly, saying in its promotional material that it can "create the world's largest, most reliable, all-hazard disaster alerting network by combining data from global institutions and data providers with crowd-sourced user accounts." Many regional apps operate this way too. For example, the government-run Safer Ohio App has a "see something send something" function, allowing users to send in information about suspicious activity or even dial 911 directly from the app. Had the SAIP app been similarly equipped, its users could have been more rapidly informed by fellow citizens, despite the delay in the official notification process.

Storing data in the app, versus online

When we did our analysis of smartphone apps for disasters, we found that many of the apps aimed at use by emergency responders did not use much communication. Rather, they were reference materials, such as guidelines for medical triage or references on infectious agents. For example, the WISER app from the National Library of Medicine is designed to assist first responders to emergencies involving

hazardous materials. It offers information about various substances from the National Library of Medicine Hazardous Substances DataBank.

However, new apps are increasingly including communication features. In addition to connecting users to each other, they can ensure reference material is up-to-date. These functions primarily rely on Wi-Fi, cellular data or Bluetooth connections. Smart app developers are including redundancy, like in the American Red Cross apps. Its Flood app, for example, lets users notify others they are safe via social media, text message and e-mail.

Creating new communications networks

Beyond building communications redundancy into apps, some companies are building systems that will allow responders and the lay public alike to communicate without cellular data or Wi-Fi. An app called FireChat, for example, can connect nearby phones directly via Wi-Fi or Bluetooth. This allows the users to create their own network.

According to FireChat's developer, Open Garden, the app can combine multiple devices to create a real network, passing a message from one to the next until it reaches the intended recipient. This type of system can be an excellent substitute in

situations where normal communications capabilities are limited.
This approach doesn't just involve smartphone applications. A device called a goTenna can connect to a smartphone via Bluetooth and communicate with other goTenna users up to several miles away. This works only between people who have goTenna devices, but is another way people can create what the company calls "people-powered" networks that do not need towers, routers or satellites. The obvious downside is that only people with the devices are able to communicate – having just one during a disaster is not enough, and in fact the company only sells them in pairs.
In addition, there are devices emergency responders use that are also available to the public. Some members of my FEMA team use a Delorme inReach Communicator, which allows users to send text messages over the global Iridium satellite network. It's expensive, but in major disasters it is a potentially valuable backup link.
When communications break down in a crisis, it's a problem for emergency responders and regular people alike. With more reliable connections, responders can be better informed about the situations they'll face, the public can be notified of ways to help and how to avoid further problems. Sadly, disasters will keep occurring. But the future is bright for improved communication when they happen. It's even possible that someday smartphones may be able to monitor the environment automatically and contribute to disaster alert systems on their own.

Nicholas Kman *is Associate Professor of Emergency Medicine, The Ohio State University.*

Accelerating Wearable Technology for First Responders

Soure: http://i-hls.com/2016/08/accelerating-wearable-technology-for-first-responders/

Aug 11 – The Center for Innovative Technology (CIT) announced the kickoff of EMERGE 2016: Wearable Technology for First Responders, a pilot program using business accelerators to speed the delivery of the latest innovative wearable technologies to responders.

The program brings together entrepreneurs, industry partners, technologists, investors, and public sector influencers working in concert to actively advance breakthrough solutions.
EMERGE is part of a larger US dept. of Homeland Security (DHS) S&T initiative to engage entrepreneurs in finding innovative ideas that address the unique needs of the Homeland Security community.
CIT, a non profit corporation, partnered to launch the program with the DHS S&T, the U.S. Dept. of Energy Pacific Northwest National Laboratory (PNNL), and TechNexus – a venture collaborative that sits at the intersection of large, incumbent corporations and the entrepreneurial ecosystem. TechNexus reaches innovators from across the global ecosystem, and builds ventures around demand-driven innovation.
The aim is to find the next round of innovative companies, to catalyze and commercially develop emerging technologies for enhanced productivity and safety for First Responders, with broad application in the public safety, utilities, construction and mining industries.

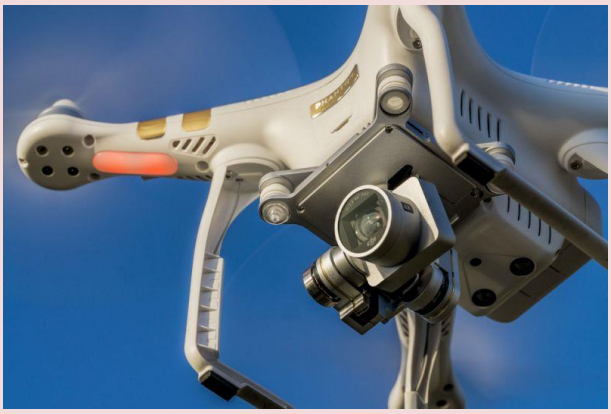
This year's program, a continuation of the successful EMERGE 2015 pilot program, invites new companies developing the next generation of wearable technologies to apply.

UAV and Video Analytics Technologies for Olympics Safety

Source: http://i-hls.com/2016/08/uav-and-video-analytics-technologies-for-olympics-safety/

Aug 10 – Securing the Olympic events in Rio encompasses the use of various technologies, according to SourceSecurity.com. Among them:

- **UAVs geofencing software** – Leading drone maker DJO introduced a new geofencing system for its drones, in order to assure that they don't disrupt the Olympics. The restrictions were added at



the request of the Brazilian military and will remain in place for the entirety of the athletic events in an effort to enhance safety and security, according to DJI announcement. Similar restrictions were incorporated into DJI's software for other large events that drew security concerns, such as the presidential nominating conventions in the U.S., the Group of Seven Summit in Japan and the Euro 2016 football tournament in France.
- **Video Analytics –** According to a security specialist, Ron Lander, "there are cameras with analytics software and network video recorders with analytics inside the engine." Users can program video analytics cameras to look for and alarm on certain kinds of video. For instance, analytics can be set to alarm when people run through a camera's field of view. Analytics can look for motion in a place and at a time when nothing should be moving. The technology can identify abandoned packages and alert security to investigate. There are a number of security scenarios that video analytics can stand in for human beings.
- The Olympic grounds have surveillance cameras as well as access control points. In addition, there are cameras connected to facial recognition systems. Indoors cameras take head on video that is required for reliable **facial recognition**. As the camera system clears people, the access control system checks them in.

At least 247 killed in earthquake in central Italy

Source: http://edition.cnn.com/2016/08/23/europe/italy-earthquake/

Aug 24 – **At least 247 people were killed after a 6.2-magnitude earthquake struck central Italy** Wednesday, according to Italy's Civil Protection Department.

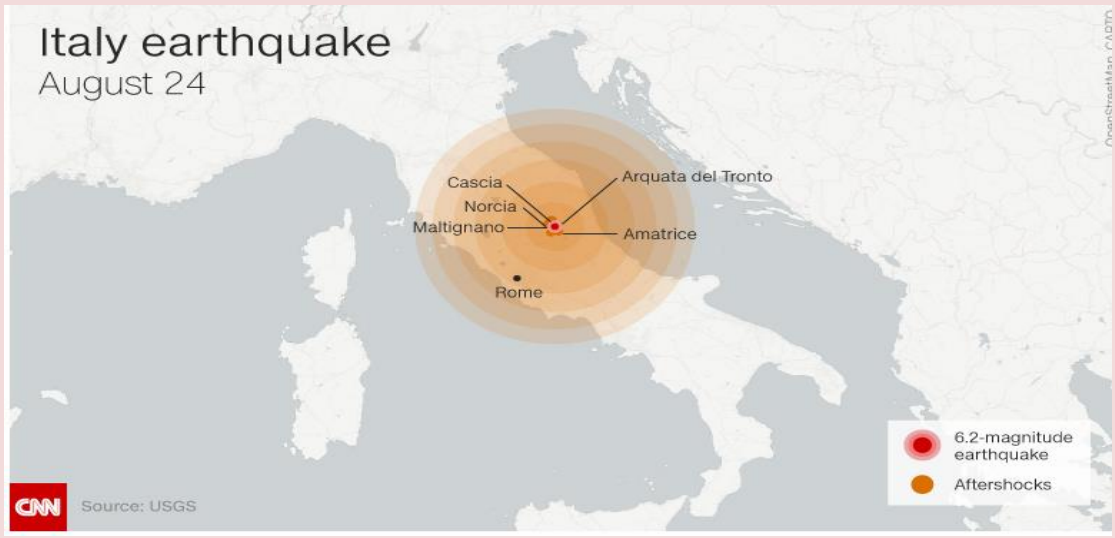
In the small Italian towns hit hard by a magnitude-6.2 earthquake that struck in the middle of the night, rescuers feverishly dug through the rubble of downed homes and apartments looking for survivors.

The powerful earthquake hit 10 kilometers (6.2 miles) southeast of Norcia at 3:36 a.m. (9:36 p.m. Tuesday ET).

Italy's Civil Protection agency said of the people killed in the quake, at least 53 of them were in the town of Amatrice, and at least 100 people were injured. Other fatalities were reported in the nearby towns of Accumoli and Arquata del Tronto.

More than 1,000 people have been displaced by the quake, and the Civil Protection agency said no residents will be allowed to sleep in the devastated town of Amatrice Wednesday night.

Amatrice 'is no more,' says mayor



The towns at the epicenter of the quake -- Amatrice, Accumoli and Arquata del Tronto -- are scenes of devastation, with what were once charming three-story buildings pancaked by the disaster.

Much of the houses in the area -- unreinforced brick or concrete frame buildings -- were vulnerable to earthquakes, according to the US Geological Survey, and offered little resistance to the powerful temblor.

Amatrice, a town of about 2,000 people in the north of Italy's Lazio region, is in ruins. But amid the rubble, the town's clock tower stood tall, with the clock stopped at the time the quake struck.

The hearts and souls of Newsletter's Team is with our Italian neighbors.
May God spare their lives and death toll remains as low as possible!

Flood-related losses in Germany to increase under climate change

Source: http://www.homelandsecuritynewswire.com/dr20160727-floodrelated-losses-in-germany-to-increase-under-climate-change

July 27 – Flood-related losses can be expected to increase considerably in Germany as a result of climate change, a new study shows. Extreme events like the severe floods along the river Elbe have already illustrated the potentially devastating consequences of certain weather conditions such as severe rainfall events, when continuing intense rain can no longer be absorbed by the soil and water levels in the rivers rise. Without appropriate adaptation, flood-related damage of currently about €500 million a year could multiply in the future, according to the comprehensive expert analysis published in the journal *Natural Hazards and Earth System Sciences*.

"Extreme events like the Elbe flood in June 2013 may be rare events, but they have major impacts on people and the environment and cause tremendous financial damage," lead author Fred Hattermann from the Potsdam Institute for Climate Impact Research (PIK) explains. PIK says that the assessment of damage is therefore of importance for local communities but also for the insurance business. Based on an earlier study on behalf of the German Insurance Association (GDV), the researchers reviewed the extent of potential flood damages and reconfirmed their original results by means of a much broader set of climate model combinations and computer simulations. "Not only does our elaborated analyses illustrate once again how flood-related damage will increase in the future, the damages costs could be even higher than previously thought," Hattermann says.

Rhine, Danube, Elbe, Weser, and Ems: 5473 river sections

"We examined in 35 different projections how the five largest river basins in Germany will be affected by climate change up until the end of this century. 5473 river sections of the Rhine, the Danube, the Elbe, the Weser and the Ems were considered," Hattermann explains. These changes in climate were transformed into changes in flood hazards and their damage potential. "It is remarkable how, despite the uncertainties that come with each scenario analysis, all new scenarios project an increase in damage. So it is all the more important to adapt to a changing climate — and there are quite a lot of possibilities to do so when it comes to floods," says co-author Olaf Burghoff, Head of Statistics (Property) and Natural Hazard Modelling of GDV.

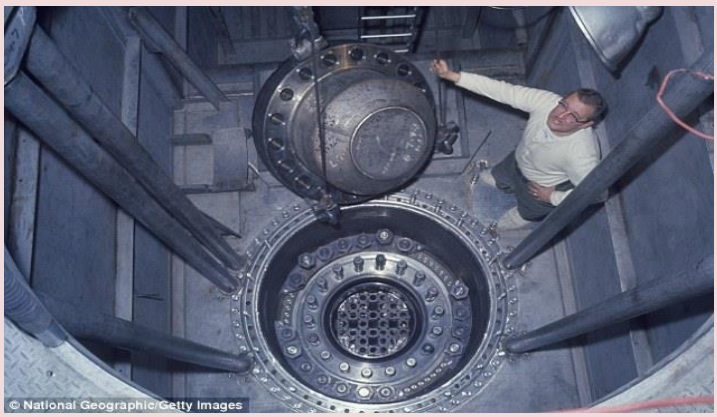
"Research is never finished, but is an ongoing process. As scientists we continuously put our work to the test in order to achieve even more robust results," co-author Peter Hoffmann from PIK says. "Here the recheck turned out to be interesting in more ways than one, because the confirmation of our results also showed that the previous estimates were too conservative." To compute the potential damage, only private houses and small enterprises were considered, but no large firms or power plants which are usually located near rivers. In reality, total economic losses can be essentially higher.

— Read more in F. F. Hattermann et al., "Brief Communication: An update of the article 'Modelling flood damages under climate change conditions — a case study for Germany'," Natural Hazards and Earth System Sciences 16 (19 July 2016): 1617-22 (doi:10.5194/nhess-16-1617-2016); and F. F. Hattermann et al., "Modelling flood damage under climate change conditions - a case study for Germany," Natural Hazards and Earth System Sciences 14 (2 December 2014): 3151-68 (DOI:10.5194/nhess-14-3151-2014).

Mysterious, ice-buried Cold War military base may be unearthed by climate change

Source: http://www.sciencemag.org/news/2016/08/mysterious-ice-buried-cold-war-military-base-may-be-unearthed-climate-change

Aug 04 – It sounds like something out of a James Bond movie: a secret military operation hidden beneath the Greenland Ice Sheet. But that's exactly what transpired at Camp Century during the Cold War.



In 1959, the U.S. Army Corps of Engineers built the subterranean city under the guise of conducting polar research—and scientists there did drill the first ice core ever used to study climate. But deep inside the frozen tunnels, the corps also explored the feasibility of Project Iceworm, a plan to store and launch hundreds of ballistic missiles from inside the ice.

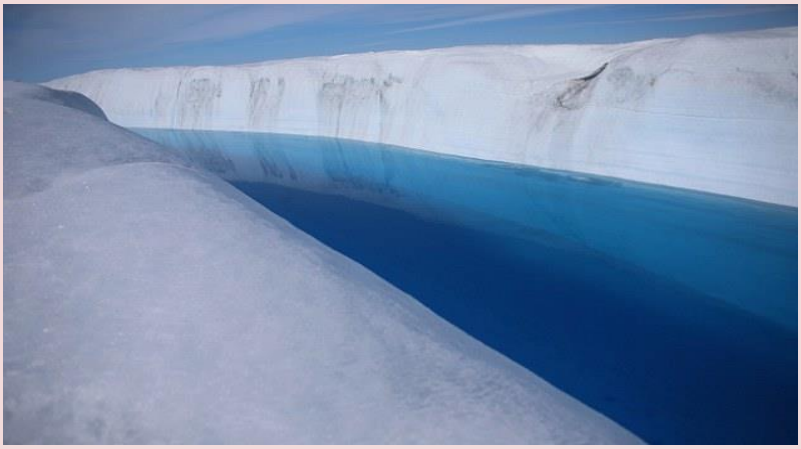
The military ultimately rejected the project, and the corps abandoned Camp Century in 1967. Engineers anticipated that the ice—already a dozen meters thick—would continue to accumulate in northwestern Greenland, permanently entombing what they left behind.

Now, climate change has upended that assumption. New research suggests that as early as 2090, rates of ice loss at the site could exceed gains from new snowfall. And within a century after that, melting could begin to release waste stored at the camp, including sewage, diesel fuel, persistent organic pollutants like PCBs, and radiological waste from the camp's nuclear generator, which was removed during decommissioning.

If these predictions come to pass, the researchers say the cleanup could create political tension between the United States and Denmark, which granted Greenland partial autonomy in 1979. The situation would also represent a new type

of climate dispute, one that offers a glimpse of the kinds of multigenerational and multinational challenges society can expect to encounter, says Liam Colgan, a glaciologist at York University in Toronto, Canada, and lead author of the study, published today in *Geophysical Research Letters*.

Colgan's team used two different combinations of regional and global climate models to estimate how conditions might change at the camp's location in the future. They considered an emission scenario in which temperatures rise 5°C by 2100. One model pair predicted that Camp Century would begin to lose ice around 2090; another suggested it could remain safe into the next century. But, Colgan says, "we would just say it's going to take longer in that scenario."



Whenever the ice does start to disappear, the researchers estimate it will take another 90 years or so for surface melting to eat through the estimated 60 meters of ice that will cover the camp by then. But meltwater percolating down through the ice sheet could pick up and wash abandoned waste downstream decades sooner.

PCBs may pose the largest danger to the environment and human health, Colgan says, and they could be abundant at Camp Century, although it's hard to know for sure. The military used paints containing up to 5% PCBs at other Arctic sites built around the same time—including the Distant Early Warning (DEW) Line radar sites that scanned for Soviet missiles coming over the pole. U.S. and Canadian authorities have already remediated much of this pollution at DEW Line stations in North America.

Camp Century also contains radiological waste, although the amount pales in comparison to the contamination unleashed by the nearby crash of a U.S. B-52 bomber in 1968. That plane was loaded with four hydrogen bombs when it went down on the sea ice near the Thule Air Base—200 kilometers west of Camp Century—releasing radioactive elements including uranium and plutonium. The United States and Denmark quickly launched project Crested Ice to contain and recover the pollution, although studies have found that some persists today.

Without any established agreement on who now bears the responsibility for cleaning up Camp Century, Colgan and his colleagues argue that the situation could strain relationships between the United States, Greenland, and Denmark. Denmark originally granted the United States permission to establish military bases there, although it's unclear whether the Danish government knew about the full scope of activities at Camp Century. Representatives of the Danish and Greenlandic governments, and U.S. military officials, did not respond to requests for comment.

"It plays into a discussion about the U.S. and Denmark using

Greenland for their own purposes, and then the Greenlandic people have to deal with it afterwards," says Kristian Nielsen, a science historian at Aarhus University in Denmark, who

was not involved in the study. Even before the construction of Camp Century and the plane crash, military operations had impacts on Greenlanders: The entire Inuit village of

Uummannaq was relocated in 1953 to make way for the construction of the Thule Air Base, about 240 kilometers west of Camp Century.

Aqqaluk Lynge, a board member and former president of the Inuit Circumpolar Council of Greenland in Nuuk, helped secure modest reparations from Denmark for the displaced residents of Uummannaq, and he says waste leaching from Camp Century would certainly be a problem. If it reaches the ocean, he says, it could impact the North Water Polynya, an ice-free area off the island's northwest coast that provides important year-round habitat for marine mammals and birds. However, Lynge says that Greenland has maintained a good relationship with the United States, and he is optimistic that Greenlandic officials and their Danish counterparts will find a way to collectively address the problem if and when it arises. "It will be a new situation that we have to find a common ground on," he says.

Colgan argues that a good first step would be to conduct more research on how climate change could affect the ice sheet and its buried hazards. But he says Denmark and North Atlantic Treaty Organization research programs both declined to support his work, despite the fact that his proposals each received favorable technical reviews. "Both rejections were fairly explicit that it was basically a touchy science topic," says Colgan, who, along with his colleagues, completed the research in his spare time.

Colgan and his co-authors aren't arguing for remediating the waste at Camp Century anytime soon—a prohibitively expensive proposition. It would only become necessary after ice melt has progressed substantially, and that may not happen as soon as the study suggests, says Ian Howat, a glaciologist at The Ohio State University, Columbus, who was not involved in the study. The new results hinge on greenhouse gas emissions increasing at an unabated pace, "which I hope is not a reasonable presumption," Howat wrote in an email.

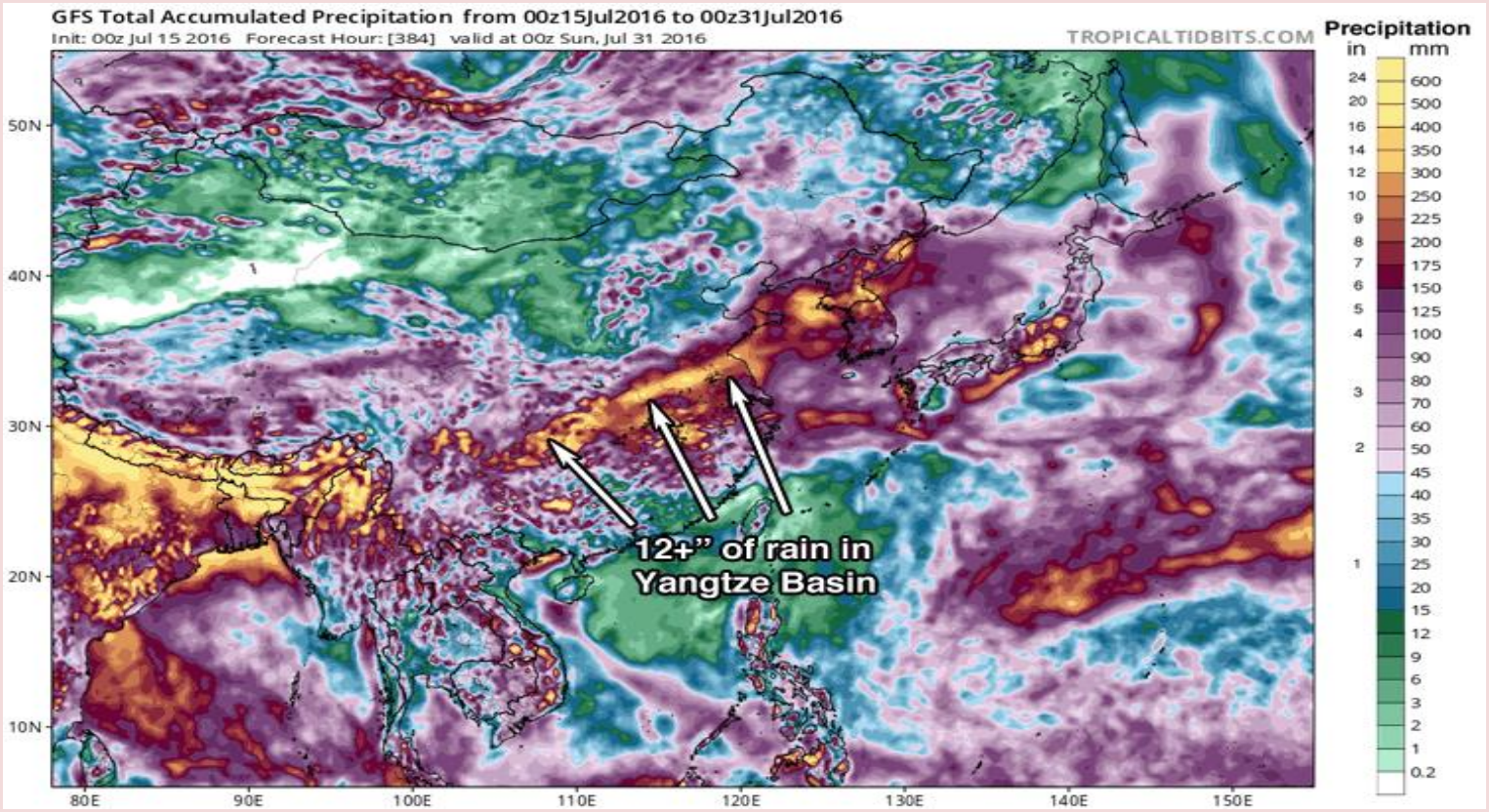
However, it's important to consider the worst-case scenario, says Miren Vizcaíno, a climatologist at the Delft University of Technology in the Netherlands. "It is very good that we have the knowledge of what would happen if we don't do anything." Some of her previous work suggests that

Camp Century could remain in the accumulation zone until at least 2100, because increasing snowfall—another consequence of climate change—may offset melting there. But that could just be temporary: The spot may eventually succumb to ice loss if warming continues, she says.

The possibility, however remote, illustrates the kinds of unexpected political conflicts that will begin to arise in a warming world, Colgan says. Sooner or later, he says, "the international community needs to develop mechanisms to deal with these sorts of thorny climate change issues."

Worst flooding since 1998 leaves $33 billion economic toll in China

Source: http://www.homelandsecuritynewswire.com/dr20160809-worst-flooding-since-1998-leaves-33-billion-economic-toll-in-china



Aug 09 – Impact Forecasting, Aon Benfield's catastrophe model development team, the other day launched the latest edition of its monthly Global Catastrophe Recap report, which evaluates the impact of the natural disaster events that occurred worldwide during July 2016. Aon Benfield is the global reinsurance intermediary and capital advisor of Aon plc.

The report reveals that much of China endured substantial seasonal "Mei-Yu" rainfall that led to a dramatic worsening of flooding along the Yangtze River Basin and in the country's northeast. Nearly twenty provincial regions were impacted by floods that have been ongoing in some areas since May. Data from China's Ministry of Civil Affairs indicated that a combined 764 people were left dead or missing, and more than 800,000 homes and other structures were damaged or destroyed.

Aon says that considerable damage to the agricultural sector was also prevalent with an estimated

eighteen million acres of cropland damaged by floodwater. **Total combined economic losses were estimated at $33 billion, with at least $28 billion occurring in the Yangtze River Basin.** The China Insurance Regulatory Commission cited insurance claims payouts representing less than 2.0 percent of the economic cost, with most of the claims from lost agriculture.

Adam Podlaha, Global Head of Impact Forecasting, said: "While it was expected that China would see above normal rainfall during the peak monsoon months with such a strong El Niño, the intensity and scope of what transpired from the associated floods were at a magnitude not seen in nearly two decades. The flood peril is one which is becoming better understood by catastrophe modelers, and the industry is better prepared than ever to help create awareness of the risks associated with such large events."

Meanwhile, the United States recorded six separate outbreaks of severe convective storms and flash flooding from the Rockies to the East Coast. Total combined economic losses were minimally estimated at $1.5 billion. By contrast to China, public and private insurers were anticipated to record losses nearing $1.0 billion or 67 percent of overall economic costs.

Many of the storms were spawned by an extended period of very hot and humid conditions that led to a "Ring of Fire" thunderstorm pattern. This active weather pattern also contributed to elevated thunderstorm and flood activity and damage in Canada's provinces of Alberta, Saskatchewan, Manitoba, Ontario, and Quebec. Total combined economic and insured losses were expected to well exceed USD100 million once all assessments are completed.

Aon notes that events to have occurred elsewhere during the month of July include:

- **Monsoon rains** also led to extensive flood damage elsewhere in Asia. More than 230 people were left dead or missing in India, Nepal, Pakistan, Indonesia and Afghanistan as tens of thousands of homes were destroyed.
- **Super Typhoon Nepartak** claimed eighty-two lives as it made separate landfalls in Taiwan and China. Though not officially coming ashore, its outer bands lashed northern portions of the Philippines. The heaviest damage was noted in Taiwan and China, where at least 38,000 homes were damaged or destroyed. Combined economic losses were at least $1.5 billion.
- **Severe thunderstorms and flash flooding left considerable damage across parts of South Africa,** killing at least seven people. The local insurance industry anticipated insured losses exceeding $145 million. Overall economic losses were much higher.
- **Tropical Storm Mirinae** made separate landfalls in southern

China and northern Vietnam, leaving at least five people dead or missing. The storm left more than 2,000 homes and 110,000 hectares (272,000 acres) of cropland damaged or destroyed. Total combined economic losses were listed at $20 million.

- **The Sand Fire** was ignited in California, charring more than 41,432 acres (16,770 hectares) of land. Two people were killed as the fire damaged or destroyed more than 140 homes and other structures.

Along with the Impact Forecasting July 2016 Global Catastrophe Recap report, users can access current and historical natural catastrophe data and event analysis on Impact Forecasting's Catastrophe Insight Web site, which is updated bi-monthly as new data become available.

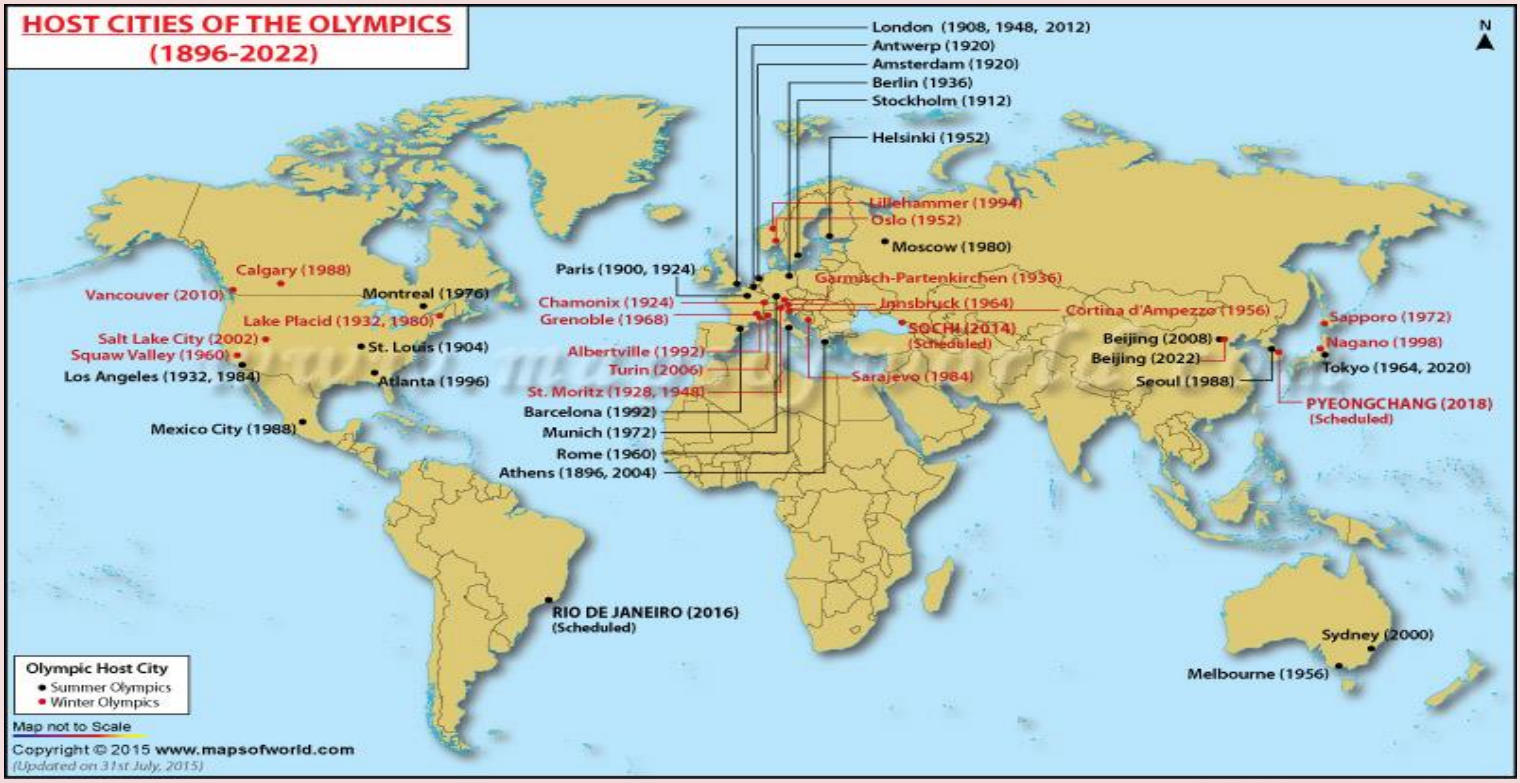
Global warming would make most cities too hot, humid to host summer Olympics

Source: http://www.homelandsecuritynewswire.com/dr20160822-global-warming-would-make-most-cities-too-hot-humid-to-host-summer-olympics

Aug 22 – Health and safety of Olympians has been an ongoing story at Summer Olympic Games. In 2008, air quality raised concerns in Beijing, while 2016 has been dogged with questions about polluted water and the Zika virus. Now**, a new commentary says the future of the summer Olympics may be in jeopardy for another reason: rising heat and humidity due to climate change.**

Among the findings, appearing in the *The Lancet* last week: By 2085, only eight Northern Hemisphere cities outside of Western Europe are likely to be cool enough to host the summer games. San Francisco would be one of just three North American cities that could serve as hosts.

The authors of the study are coauthored by UC Berkeley public health professors



Kirk Smith and John Balmes, Alistair Woodward of the University of Auckland, and Cindy Chang, the physician in charge of UC Berkeley's athletic teams and the chief medical officer for Team USA at the 2012 London Olympics.

UC Berkeley says that in the commentary, which comes from a larger study about climate change, the authors explain how their findings can be used to examine the viability of future Olympic sites based on a measurement that combines temperature, humidity, heat radiation, and wind — their wetbulb globe temperature (WBGT). Researchers used two climate models to project rising temperatures over the next century and applied those results to current safety procedures used in determining the viability of a host city.

The final study, which is still forthcoming and holds much broader implications than the future of outdoor Olympics, examines the relationship between health and productivity as the global climate continues to warm. The opening ceremonies of the 2016 games in Rio, however, did acknowledge climate change, and the impact that rising temperatures could have on the future of the games was not lost on Smith and his colleagues.

"Climate change could constrain the Olympics going forward," said Smith, a professor of global environmental health in the School of Public Health. "And not just because of rising sea levels."

The findings focused on the Northern Hemisphere, home to 90 percent of the world's population. The authors considered only cities with at least 600,000 residents, the size considered necessary for hosting the games. Cities with elevations over a mile above sea level were omitted, as the most recent Olympic games hosted at such an altitude (Mexico City in 1968) faced challenges of their own.

The findings assumed that any venue with more than a 10 percent chance of having to cancel a marathon — one of the summer Olympics' signature and exclusively outdoor events — on short notice would not be a viable host city.

"If you're going to be spending billions of dollars to host an event, you're going to want have a level of certainty that you're not going to have to cancel it at the last minute," Smith said.

The 10 percent criterion is currently used to evaluate potential sites of the winter games. If a potential host city is too unlikely to produce enough snow or cold enough temperatures, the chances of its bid winning decreases.

The findings indicate that by 2085, Istanbul, Madrid, Rome, Paris, and Budapest – all cities that are or were in contention for either the 2020 or 2024 Summer Olympics – would be unfit to host the games. Tokyo, the city that has secured the 2020 summer Olympiad, would also be too hot to ensure athlete safety, should these projections come to pass.

According to the findings, eight out of 543 cities outside of Western Europe would qualify as "low-risk" sites, including St. Petersburg, Russia; Riga, Latvia; Bishkek, Kyrgyzstan; and Ulaanbaatar, Mongolia.

In North America, Calgary and Vancouver would join San Francisco as the only three suitable sites. Both Canadian cities have hosted Olympics before — but the winter games, Calgary in 1988 and Vancouver in 2010. San Francisco explored the possibility of hosting this year's summer games, but ultimately withdrew the bid in 2006.

Latin America and Africa combined would fail to provide a single viable city.

Western Europe is home to twenty-five cities that would be "low-risk" sites in 2085, according to the calculations.

But by the twenty-second century, if their projections play out, the scientists concluded that only four Northern Hemisphere cities would be left on the list: Belfast and Dublin, Ireland; and Edinburgh and Glasgow in Scotland.

While these findings are concerned with the more distant future, being able to ensure athlete safety in the face of spiking temperatures is already an issue in outdoor summer competitions. In October 2007, the Chicago Marathon was canceled mid-race as hundreds of runners succumbed to the heat and sought medical attention. High temperatures also wreaked havoc this year during the U.S. Olympic Team trials marathon in Los Angeles, where 30 percent of the Olympic hopefuls failed to finish as the temperature on race day pushed 80 degrees Fahrenheit.

Should the findings reported in this commentary bear out, obvious work-arounds exist, such as running the Olympics indoors entirely or eliminating heat-sensitive endurance events like the marathon. Both solutions, however, would require a dramatic reimagining of how the modern Olympics are constructed.

"Climate change is going to force us to change our behavior from the way things have always been done," said Smith. "This includes sending your kids outside to play soccer or going out for a jog. It is a

substantially changing world. If the world's most elite athletes need to be protected from climate change, what about the rest of us?"

— Read more in Kirk R Smith et al., "The last Summer Olympics? Climate change, health, and work outdoors," The Lancet 388, no. 10045 (13 August 2016): 642–44.