2 CBRNE DIARY

Dedicated to Global First Responders

CBRNE-Terrorism Newsletter

November 2018

www.cbrne-terrorism-newsletter.com

ICI International CBRNE INSTITUTE

CBRNE-Terrorism Newsletter

W O M D

C²BRNE DIARY

DIRTY R-NEWS

Fukushima's Nuclear Imprint Is Found in California Wine

Source: https://www.nytimes.com/2018/07/20/science/fukushima-radiation-levels-california-wine-nyt.html

July 2018 – Ever since a huge earthquake off the coast of Japan sent a tsunami crashing into a nuclear plant in Fukushima, setting off one of the world's worst nuclear crises, scientists have been uncovering the radioactive legacy of the 2011 disaster.

The government warned about contaminated seafood around Japan, and toxic water, sludge and rubble. More frighteningly, radioactive wild boars marauded Japanese towns and attacked people.

Now a group of French nuclear physicists say they have stumbled on Fukushima's signature in Northern California wine. (No, it's not believed to be dangerous — more on that later.)

In a **new study,** the researchers report testing 18 bottles of California rosé and cabernet sauvignon from 2009 onward and finding increased levels of radioactive particles in the wine produced after the Fukushima disaster. In the case of the cabernet, the levels of the radioactive materials doubled.

EDITOR'S COMMENT: In the title there was also a parenthesis writing "Drinkers do not panic" – meaning what? That cesium is good for our health? On the other hand, the article writes about "French" nuclear scientists – what a coincidence! France is also a prominent Cabernet Sauvignon producer! But who am I to say? I prefer "ouzo"!

Nuclear counter terror detection systems to be bolstered in high-tech drive

Source: https://www.telegraph.co.uk/news/2018/10/20/nuclear-counter-terror-detection-systems-bolstered-high-tech/

Oct 20 – Counter-terrorism officers are to be equipped with a new fleet of high-tech nuclear and radiological detection vehicles to trace weapons-grade materials in the UK.

The Home Office is planning to buy up to 10 mobile gamma and neutron radiation detection systems to bolster its defences against them being used in a terror attack.

Ports and airports across the country already have screening systems in place to spot anyone smuggling nuclear or radiological materials into the UK as part of the Border Force's Cyclamen monitoring system. Similar equipment was used at the Olympic Park during the 2012 Summer Olympics in London.

But, the new fleet is understood to be able to carry out searches for such materials inland and be deployed with speed at key locations.

A Home Office source insisted that the threat of such materials being used in a so-called dirty bomb terror attack remained "highly unlikely".

However, in 2006 Russian agents were accused of smuggling in polonium 210, a highly radioactive chemical, to poison fatally the former KGB agent Alexander Litvinenko.

A procurement notice, lodged last month, states that ministers are inviting bids for between five and 10 "modern vehicle-based gamma and neutron radiation detection systems for various national security and radiological and nuclear counter-terrorism activities."

Statistics held by the International Atomic Energy Agency shows that in 2016 there were 189 incidents of nuclear materials being discovered outside of state control. That compares to 147 such reports made to the agency five years earlier.

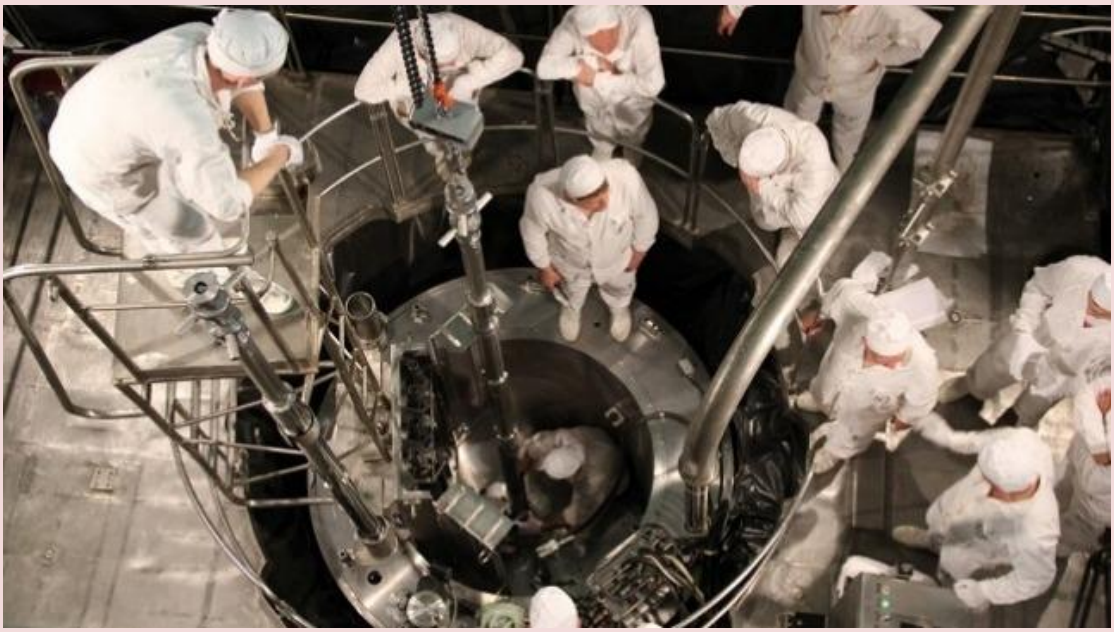
While those reports will include illegally trafficked materials, it will also log scrap metal contaminated with radiological materials after being broken up.

This summer, the Government published its counter-terrorism strategy, called CONTEST, in which it underlined its commitment to "refreshing" defences with new technologies to "enhance our detection and

screening capabilities, for example at borders, airports and crowded places".
The report, released following the Manchester and London terror attacks, highlighted the need for "cutting-edge" detection system that "can be flexibly deployed in a range of environments."
The report adds: "We will deliver this through investment in modern systems, informed by the latest science and technology research and international collaboration."
A Home Office spokesperson said: "This procurement activity relates to the CONTEST commitment to continue to strengthen the UK's existing radiological and nuclear detection capabilities. It does not relate to chemical or biological materials.
"This particular activity is not in response to a specific threat. The use of radiological or nuclear materials in an attack by terrorists remains significantly less likely than a conventional or chemical attack."
He refused to be drawn on the possible cost of the vehicles.

First Reactor Started on Russia's Floating Nuclear Plant

Source: https://www.maritime-executive.com/editorials/first-reactor-started-on-russia-s-floating-nuclear-plant



Technicians loading the first reactor aboard the Akademik Lomonosov, Russia's floating nuclear power plant. Credit: Rosenergoatom

Nov 05 – Russia's floating nuclear power plant, long a controversial dream of the country's atomic energy industry, has finally become an actual nuclear power plant after its first reactor achieved a sustained chain reaction at its mooring in Murmansk harbor last week.
The news came in a release to RIA Novosti, a semi-official Russian newswire, which on Friday quoted an unnamed official with Rosatom, Russia's state nuclear energy enterprise.
"The physical launch of the reactor unit on the starboard side of the floating power plant Akademik Lomonosov occurred on Friday," the official was quoted as saying.
"The reactor unit reached the minimum controlled power level at 17:58 Moscow time."
A series of reactor tests will now follow, according to the official, and the second reactor on the port side of the nuclear barge will be brought to minimum power in the coming days.
After the reactor tests, the *Akademik Lomonosov* will be towed through the Arctic to the far eastern Siberian port of Pevek, a town of 100,000 people in Chukotka, were it is slated to go online in the summer of 2019. The plant is expected to replace the energy supplied by the Bilibino nuclear power plant – the world's four northernmost commercial reactors – which Rosatom will begin decommissioning in 2021.

For 12 years Russia has been pursuing its audacious experiment in floating nuclear power, fording a river of doubt, economic downturns and environmental outcry – and confounding critics who said the plant was an expensive publicity stunt that was doomed to failure.
Despite dodging such predictions, the plant remains as improbable as ever – a huge, ungainly nuclear solution in search of a problem.

Since its rocky – and often secretive – beginnings in the early 2006, Russia has attempted to sell the plant as a cure-all for energy woes in the world's more remote regions.
And while the plant has spawned a number of imitation plans in other coutries, it has failed to draw the windfall of orders Rosatom said would justify its $480 million cost. Rosatom officials themselves have conceded that this price tag is too high to bring the floating plant, as designed now, into serial production.
Yet the corporation has done much in recent months to draw back the veils of mystery it draped over the plant through much of its construction. The apprehensive eyes of the world's media were upon the plant last April when it was finally towed into the open ocean from St Petersburg's Baltic Shipyard en route to Murmansk.
In October, Rosatom invited Bellona to be the first foreign environmental group to inspect the *Akademik Lomonosov* at its moorings at Atomflot, Russia's Murmansk-based nuclear icebreaker port.
Still, the new openness has done little to settle Bellona's central concerns about Rosatom's long-range intentions for its floating nuclear power plant. By design, the plant is meant to operate in remote regions. But this very remoteness, Bellona has said, would vastly complicate the rescue operations that would be necessary after an accident, as well as the more routine clearing of spent nuclear fuel from its reactors.
Likewise, visions of Fukushima's waterlogged reactors have not faded from public memory, and the thought of a nuclear power plant as vulnerable to tsunamis and foul weather as is the ocean-based *Akademik Lomonosov* strikes an anxious chord among environmentalists.
Rosatom has often said the plant is invulnerable to tsunamis and cites the fact that its water-borne location will give it access to infinite supplies of reactor coolant in the event of an accident.
But environmentalists are skeptical. In the worst-case scenario, the plant might not ride out the waves, but instead be torn from its moorings to barrel inland through buildings and towns until it lands, battered and breached, with two active nuclear reactors on board – well away from its source of emergency coolant.
Rosatom's best option in that disaster scene would be the 24-hours worth of backup coolant located aboard the barge, which is hardly reassuring.

Still, the whole idea of a floating nuclear plant has piqued curiosity – and competition. Two state-backed companies in China are said to be pursing plans for at least 20 floating nuclear plants, and American scientists have drawn up blueprints of their own.

The company estimates each floating plant will take four years to build, compared with a decade or so for standard land-based nuclear plants. The Sudan Tribune has cited that country's minister of water resources and electricity as saying the government in Khartoum has a deal to become the first foreign floating plant customer.

Nuclear experts: Archive shows that Iran had "advanced capabilities" to produce nukes

Source: http://www.homelandsecuritynewswire.com/dr20181114-nuclear-experts-archive-shows-that-iran-had-advanced-capabilities-to-produce-nukes

Nov 14 – The documents in an archive seized by Israel show that Iran had "more advanced capabilities to make nuclear weapons themselves," according to a paper being prepared by an anti-proliferation think tank, *Foreign Policy* reported Tuesday.

Foreign Policy, which saw an early draft of the paper being produced by the Institute for Science and International Security — written by the Institute's president, former weapons inspector David Albright, former Deputy Director General of the International Atomic Energy Agency (IAEA), and Andrea Stricker, a senior policy analyst at the institute — reported that the information contained in the archive "demonstrates that Washington and the IAEA were constantly underestimating how close Tehran was to a bomb."

Though the deal was meant to limit Iran's ability to highly enrich uranium to fuel a nuclear bomb, the archive shows that Iran had also developed the capabilities "to make the nuclear weapons themselves." This aspect of the archive is described as "a surprising and troubling finding in the new intelligence."

"The archive is littered with new stuff about the Iranian nuclear weapons program," Albright said. "It's unbelievable how much is in there." Based on what he has learned from reviewing the documents in the archive, he said that the Iranians "were further along than Western intelligence agencies realized."

Albright noted that though the United States government believed that it would take Iran two years to build a nuclear weapon, "the information in the archive makes it clear they could have done it a lot quicker."

The documents and files that Israel smuggled out of Tehran in January, and which Israeli Prime Minister Benjamin Netanyahu publicized at the end of April, consists of some 100,000 pages and covers Iran's nuclear weapons program during the years of 1999 to 2003.

The haul is so massive that Albright said that "I don't think even the Israelis have gone through it all." He added that "every day when they go through it they see something new."

In a previous paper published by the institute, Albright, Heinonen, and Frank Pabian, a former United Nations Nuclear Chief Inspector in Iraq for the IAEA, argued that the new information contained in the archive "necessitates calling for more action by the IAEA and the Joint Commission, which administers the Joint Comprehensive Plan of Action (JCPOA)."

In an op-ed published last month in The Hill, Josh Block, the President and CEO of The Israel Project, noted that the IAEA had failed to follow through on the recent Israeli revelations and the implications of those failures on the agency's overall knowledge of Iran's nuclear weapons work.

"The gaps in the IAEA's knowledge — of Iran's past nuclear work, of its military sites, of items mentioned in Section T of the nuclear deal, and of the nuclear sites discovered by Israeli intelligence — raise questions about the full extent of Iran's nuclear program," Block argued.

— Read more in David Albright et al., Breaking Up and Reorienting Iran's Nuclear Weapons Program - Iran's Nuclear Archive Shows the 2003 Restructuring of its Nuclear Weapons Program, then called the AMAD Program, into Covert and Overt Parts (ISIS, November 2018).

Why the security of nuclear materials should be focus of US-Russia nuclear relations

By Andrew W. Reddie and Bethany L. Goldblum

Nov 13 – The Trump administration's decision to withdraw from the INF Treaty following years of Russian noncompliance is the most recent upset in a series of escalating tensions between the two superpowers. The political status of Ukraine and Crimea, Russian disinformation campaigns in the 2016 election cycle, and continued uncertainty surrounding the extension of New START have led many commentators—even Russian Prime Minister Dmitry Medvedev—to argue that relations between Russia and the United States are at their lowest ebb since the end of the Cold War. While the Helsinki summit may have left much to be desired in terms of strategic stability and arms control, the United States and Russia need to—and can—find a balance between competition and cooperation, particularly with regard to nuclear security.

A billet of highly enriched uranium that was recovered from scrap processed at the Y-12 National Security Complex Plant.

Past efforts to bolster nuclear security—the prevention and detection of unauthorized access to and illicit transfer of nuclear and radioactive material—via four US-sponsored Nuclear Security Summits provided a starting point for securing nuclear materials around the world. But these discussions have, unfortunately, been abandoned. The United States, Russia, and a number of other countries have continued cooperating within existing institutional arrangements, such as the International Atomic Energy Agency's International Nuclear Security Advisory Service. Even so, the Nuclear Threat Initiative (NTI) and the Economist Intelligence Unit (EUI) have, for the first time, pointed to an increase in nuclear insecurity due to a "deterioration of political stability and governance, an increase in corruption, and the expanding presence of terrorist groups around the world." Moreover, the existing institutional architecture exempting some types of nuclear material—particularly material designated for use in naval propulsion—from oversight has become a growing cause for concern.

The pressing need for global action on nuclear security may offer the United States and Russia a way around the generally deteriorated state of their relations. They have, after all, both historically played key roles in creating and maintaining cooperative frameworks to bolster nuclear material security—in spite of other disagreements. Indeed, Russia and the United States are still partners in the Global Initiative to Combat Nuclear Terrorism, a collective dedicated to improving the accounting and control of nuclear materials. Future cooperation on nuclear material security would build upon numerous previous joint efforts to reduce the risks posed by fissile material, typified by the recently concluded Megatons to Megawatts Program, an effort so effective that roughly one in 10 US light bulbs was powered by fissile material from dismantled Russian nuclear weapons for multiple decades.

Today, a new framework is needed to tackle risks posed by nuclear material in transit, to track small quantities of fissile material used in testing equipment, and to address the approximately 150 metric tons of weapons-grade uranium fuel designated for use in naval propulsion.

Nuclear material security in the naval sector represents an increasingly salient issue for all states—particularly as a number of governments announce plans to develop nuclear navies or face pressure to do so. Tony Abbott, a former prime minister of Australia, argues that a nuclear naval program is necessary to address the future security challenges in his country's part of the world. South Korea has a similarly renewed interest in a nuclear navy. In the Middle East, Iran is purported to be planning a reactor for nuclear propulsion and in South America, Brazil has had an active program to develop nuclear-powered attack submarines for more than a decade. Beyond the planning phase, India recently commissioned its first nuclear submarine, the *INS Arihant*, using a Russian design.

The combination of these developments suggests that the time is ripe to consider how to decrease the proliferation and nuclear security risks associated with naval nuclear material as part of a more general reinvigoration of nuclear security practices.

Under the existing institutional architecture afforded by the Nuclear Non-Proliferation Treaty (NPT), comprehensive safeguards agreements provide a legally binding method of deterring the diversion of nuclear materials to illicit use. But safeguards agreements have two problems. First, they do not apply to all states. Countries recognized as "nuclear-weapon states" under the treaty—the United States, Russia, China, France, and the United Kingdom—are not subject to the system of inspections and audits these safeguards provide. Also, states not party to the NPT, including India, Pakistan, and North Korea, are not subject to safeguards. Then again, under the IAEA's rules, non-nuclear-weapon states can request that nuclear material they produce indigenously or without explicit supplier restrictions be exempted from safeguards—for use as (for example) fuel in naval reactors.

There are a number of potential institutional configurations for plugging the holes in the nuclear security system. One approach might involve further bolstering the cooperative measures included in the Convention on the Physical Protection of Nuclear Material—the only legally binding document that outlines government obligations to protect nuclear facilities and nuclear material in transit. Another proposal calls for a so-called Supplemental Protocol within an IAEA-supported and state-sponsored committee process. The benefit of both of these approaches is that their implementation would use the IAEA's institutional framework (relying on expertise and legal precedence emanating from the existing safeguards regime) rather than starting from scratch. A third approach may involve using the Global Initiative to Combat Nuclear Terrorism as a diplomatic vehicle to pioneer an international materials accountancy system similar to those that national governments use to keep track of their fissile material. The creation or strengthening of institutions to address nuclear material security in any of these ways would not only lessen the chance that terrorists or other bad actors could gain possession of enough fissile material to make a nuclear weapon. Improving nuclear security might also represent an opportunity to reinvigorate international cooperation on nuclear nonproliferation and arms control.

Those who do not favor major new approaches to nuclear security put forward three main arguments. The first: The risks to nuclear security are not high enough to justify intervention. Non-nuclear weapons states, for example, are years from developing nuclear navies (if they ever do so). Second, they argue that any attempt to institutionalize a universal approach to nuclear materials held by non-nuclear weapons states, nuclear weapons states, and the states that are not part of the NPT would be unwieldy and potentially legitimize nuclear proliferation in countries outside the existing NPT framework. The final argument is perhaps the most cynical, suggesting that the exemptions in the existing safeguards regime are driven, in large part, by the major powers' interest in exempting sensitive military technology from IAEA—and subsequently foreign—oversight.

Clearly, though, the arguments for dealing more effectively with nuclear security are compelling. There are a variety of international regimes involving countries that do and do not have nuclear weapons, as well as states outside the NPT framework. These include the Comprehensive Test Ban Treaty Organization, the Additional Protocol for IAEA safeguards, and the Nuclear Suppliers Group. Indeed, the need to enhance nuclear security in non-NPT countries is particularly acute; there are clear opportunities to decrease proliferation and security risks by expanding the extant safeguards architecture.

Two points should be made here. The first is that there are certainly parts of the nuclear fuel cycle that are going to remain off-limits from international oversight. Second, recent developments in theory and methods for nuclear-warhead verification offer promise for nuclear safeguards in the naval sector. Nascent work on zero-knowledge protocols, blockchain-based systems, and increasingly sophisticated remote-sensing tools such as applied antineutrino

technologies are worth further consideration as part of new nuclear-material verification and safeguards efforts to bolster nuclear security.

In simple terms, nuclear security risks are greatest where safeguards end. As the amount of nuclear material outside of the existing international safeguards architecture expands, the threat of malicious actors acquiring and weaponizing fissile material increases. Indeed the sheer mass of naval nuclear material in the United States and Russia calls into question the limits of safety. A US-Russian-led effort to deal with naval and other nuclear materials offers the promise of addressing this key challenge. It also could provide a pathway to continued cooperation between the world's leading nuclear nations on matters that extend far beyond nuclear materials security.

Andrew Reddie *is a doctoral candidate in the Charles and Louise Travers Department of Political Science at the University of California, Berkeley. He currently serves as deputy director for the Nuclear Policy Working Group and as a researcher for the Department of Nuclear Engineering and the Goldman School of Public Policy at UC Berkeley. He is also an affiliated researcher at the Center for Long-Term Cybersecurity at the UC Berkeley Information School and the Nuclear Science and Security Consortium. He holds an MPhil in International Relations from Oxford University as well as an M.A. and a B.A. (hons.) from the University of California, Berkeley. Prior to joining UC Berkeley, he served as managing editor at the Canadian International Council and as an associate at the Council on Foreign Relations in Washington, DC.*

Bethany L. Goldblum *is an associate research engineer in the Department of Nuclear Engineering at the University of California, Berkeley and executive director of the Nuclear Science and Security Consortium, a multi-institution initiative established by the Department of Energy's National Nuclear Security Administration to conduct research and development supporting the nation's nonproliferation mission while expanding the talent pipeline. Her research focuses on fundamental and applied nuclear physics, neutron detection, scintillator characterization, multi-source analytics, and nuclear security policy. Goldblum also founded and directs the Nuclear Policy Working Group, an educational programming effort focused on developing policy solutions to strengthen global nuclear security. She is director of the Public Policy and Nuclear Threats Boot Camp at the Institute on Global Conflict and Cooperation. Goldblum received a PhD in nuclear engineering from the University of California, Berkeley.*

California fire near nuclear accident site

By John Mecklin

Source: https://thebulletin.org/2018/11/california-fire-near-nuclear-accident-site/

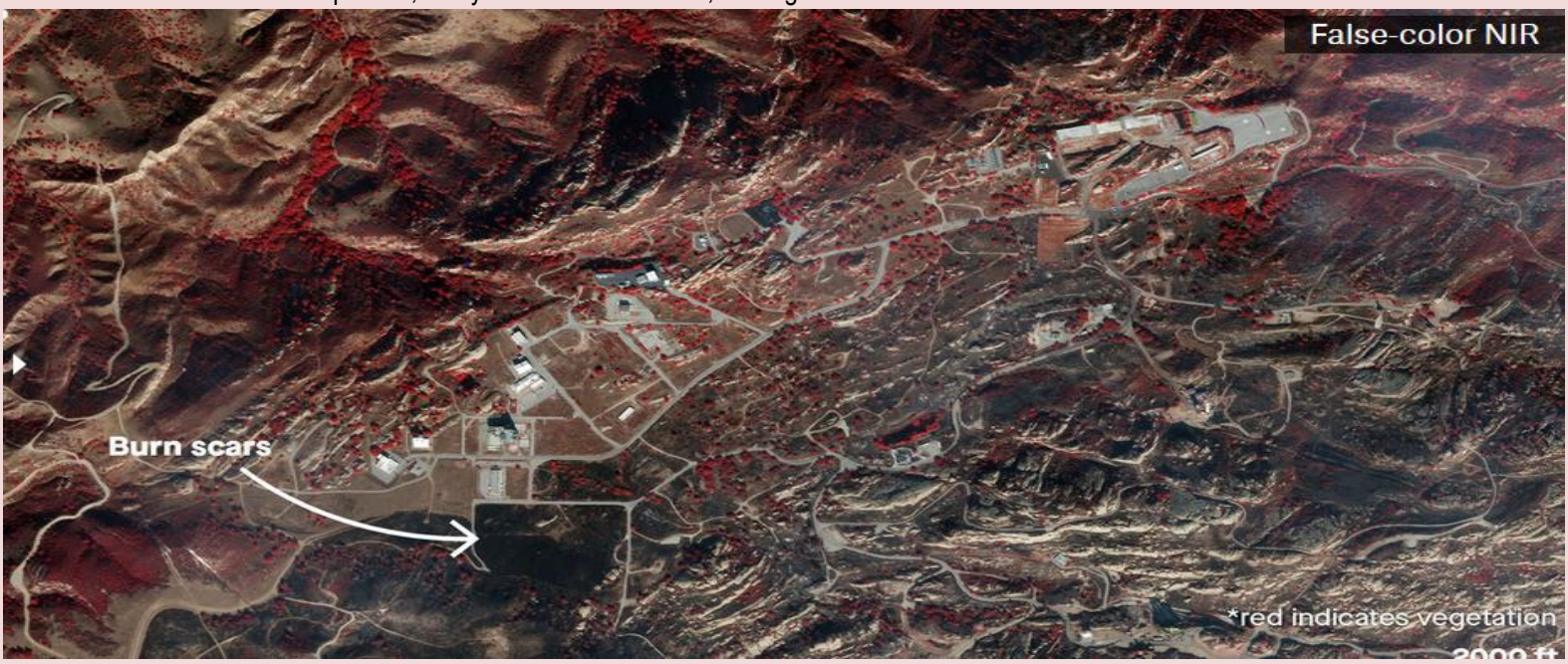
Nov 14 – Call it another sad chapter in the long and depressing book of governmental failures to properly clean up after nuclear research and production efforts. Last week, the Woolsey Fire—one of three major, climate change-charged conflagrations now afflicting California—apparently started on the grounds of the Santa Susana Field Laboratory, located just south of Simi Valley and west of Los Angeles. Closed in 1996, the lab site was home to rocket engine and nuclear reactor research; one of the nuclear efforts—the Sodium Reactor Experiment—led to the partial melt-down of a reactor in 1959 and the release of radioactive material. But as the Los Angeles Chapter of Physicians for Social Responsibility noted, the Santa Susana site is contaminated in a variety of ways: "Decades of nuclear and rocket-engine testing activity, including nuclear reactor accidents and other toxic spills and releases, have resulted in widespread contamination throughout [lab's] 2,850-acre facility."

The start of the Woolsey Fire. Credit: CBS LA

The California Department of Toxic Substances Control (DTSC) quickly announced that it didn't believe the fire had released significant amounts of toxins. "Our staff were able to access the site Saturday morning and assess damage caused by the fire," a Tuesday press release said. "We confirmed that the [lab] facilities that previously handled radioactive and hazardous materials were not affected by the fire. Over the weekend our multi-agency team took measurements of radiation and hazardous compounds, both on the site and in the surrounding community. The results from this initial round of testing showed no radiation levels above background levels, and no elevated levels of hazardous compounds other than those normally present after a wildfire."

Safecast, an international, volunteer-centered organization formed in the wake of the Fukushima Daiichi nuclear disaster, reported Wednesday that it "had no survey data from

the immediate [lab] area prior to the fire, but we had a fair amount of data from nearby communities which showed it to be at normal background levels. Our real-time radiation and particulate sensors in the Southern California region, the closet of which is 30km (about 18 miles) away from [the site], have shown no measurable increases in radiation. Safecast volunteers are on the way to the site, however, so hopefully we will have new data to share soon. Though CalFire indicates that the fire danger in the [lab] area has passed, many roads are still closed, making access difficult."



With near-infrared imagery, dense vegetation appears red while burn scars from the Woolsey fire contrast as dark brown. https://qz.com/1461195/did-the-woosley-fire-disturb-a-nuclear-waste-site-california-says-no-and-a-group-of-doctors-say-yes/

Local activists were not shy about voicing in their disbelief in governmental pronouncements about contamination and the fire. "We can't trust anything that DTSC says," West Hills resident Melissa Bumstead said. "DTSC repeatedly minimizes risk from [the lab] and has broken every promise it ever made about the [lab] cleanup. The public has no confidence in this troubled agency."
Should it? The Santa Susana Field Laboratory closed 22 years ago, and cleanup efforts remain in the planning stages.
"The Woolsey Fire likely released and spread radiological and chemical contamination that was in [the Santa Susana Field Laboratory's] soil and vegetation via smoke and ash," said Bob Dodge, president of Physicians for Social Responsibility-Los Angeles. "All wildfire smoke can be hazardous to health, but if [the lab] had been cleaned up long ago as DTSC promised, we'd at least not have to worry about exposure to dangerous radionuclides and chemicals as well."

John Mecklin *is the editor-in-chief of the* Bulletin of the Atomic Scientists. *Previously, he was editor-in-chief of* Miller-McCune *(since renamed* Pacific Standard*), an award-winning national magazine that focused on research-based solutions to major policy problems. Over the preceding 15 years, he was also: the editor of* High Country News, *a nationally acclaimed magazine that reports on the American West; the consulting executive editor for the launch of* Key West, *a regional magazine start-up directed by renowned magazine guru Roger Black; and the top editor for award-winning newsweeklies in San Francisco and Phoenix. In an earlier incarnation, he was an investigative reporter at the* Houston Post *and covered the Persian Gulf War from Saudi Arabia and Iraq. Writers working at his direction have won many major journalism contests, including the George Polk Award, the Investigative Reporters and Editors certificate, and the Sidney Hillman Award for reporting on social justice issues. Mecklin holds a master in public administration degree from Harvard's Kennedy School of Government.*

Will disruptive technology cause nuclear war?

By Matthew Kroenig and Bharath Gopalaswamy

Source: https://thebulletin.org/2018/11/will-disruptive-technology-cause-nuclear-war/

Nov 12 – Recently, analysts have argued that emerging technologies with military applications may undermine nuclear stability (see here, here, and here), but the logic of these arguments is debatable and overlooks a more straightforward reason why new technology might cause nuclear conflict: by upending the existing balance of power among nuclear-armed states. This latter concern is more probable and dangerous and demands an immediate policy response.

For more than 70 years, the world has avoided major power conflict, and many attribute this era of peace to nuclear weapons. In situations of mutually assured destruction (MAD), neither side has an incentive to start a conflict because doing so will only result in its own annihilation. The key to this model of deterrence is the maintenance of secure second-strike capabilities—the ability to absorb an enemy nuclear attack and respond with a devastating counterattack.

Recently analysts have begun to worry, however, that new strategic military technologies may make it possible for a state to conduct a successful first strike on an enemy. For example, Chinese colleagues have complained to me in Track II dialogues that the United States may decide to launch a sophisticated cyberattack against Chinese nuclear command and control, essentially turning off China's nuclear forces. Then, Washington will follow up with a massive strike with conventional cruise and hypersonic missiles to destroy China's nuclear weapons. Finally, if any Chinese forces happen to survive, the United States can simply mop up China's ragged retaliatory strike with advanced missile defenses. China will be disarmed and US nuclear weapons will still be sitting on the shelf, untouched.

If the United States, or any other state acquires such a first-strike capability, then the logic of MAD would be undermined. Washington may be tempted to launch a nuclear first strike. Or China may choose instead to use its nuclear weapons early in a conflict before they can be wiped out—the so-called "use 'em or lose 'em" problem.

According to this logic, therefore, the appropriate policy response would be to ban outright or control any new weapon systems that might threaten second-strike capabilities.

This way of thinking about new technology and stability, however, is open to question. Would any US president truly decide to launch a massive, bolt-out-of-the-blue nuclear attack because he or she thought s/he could get away

with it? And why does it make sense for the country in the inferior position, in this case China, to intentionally start a nuclear war that it will almost certainly lose? More important, this conceptualization of how new technology affects stability is too narrow, focused exclusively on how new military technologies might be used against nuclear forces directly.

Rather, we should think more broadly about how new technology might affect global politics, and, for this, it is helpful to turn to scholarly international relations theory. The dominant theory of the causes of war in the academy is the "bargaining model of war." This theory identifies rapid shifts in the balance of power as a primary cause of conflict.

International politics often presents states with conflicts that they can settle through peaceful bargaining, but when bargaining breaks down, war results. Shifts in the balance of power are problematic because they undermine effective bargaining. After all, why agree to a deal today if your bargaining position will be stronger tomorrow? And, a clear understanding of the military balance of power can contribute to peace. (Why start a war you are likely to lose?) But shifts in the balance of power muddy understandings of which states have the advantage.

You may see where this is going. New technologies threaten to create potentially destabilizing shifts in the balance of power.

For decades, stability in Europe and Asia has been supported by US military power. In recent years, however, the balance of power in Asia has begun to shift, as China has increased its military capabilities. Already, Beijing has become more assertive in the region, claiming contested territory in the South China Sea. And the results of Russia's military modernization have been on full display in its ongoing intervention in Ukraine.

Moreover, China may have the lead over the United States in emerging technologies that could be decisive for the future of military acquisitions and warfare, including 3D printing, hypersonic missiles, quantum computing, 5G wireless connectivity, and artificial intelligence (AI). And Russian President Vladimir Putin is building new unmanned vehicles while ominously declaring, "Whoever leads in AI will rule the world."

If China or Russia are able to incorporate new technologies into their militaries before the United States, then this could lead to the kind of rapid shift in the balance of power that often causes war.

If Beijing believes emerging technologies provide it with a newfound, local military advantage over the United States, for example, it may be more willing than previously to initiate conflict over Taiwan. And if Putin thinks new tech has strengthened his hand, he may be more tempted to launch a Ukraine-style invasion of a NATO member.

Either scenario could bring these nuclear powers into direct conflict with the United States, and once nuclear armed states are at war, there is an inherent risk of nuclear conflict through limited nuclear war strategies, nuclear brinkmanship, or simple accident or inadvertent escalation.

This framing of the problem leads to a different set of policy implications. The concern is not simply technologies that threaten to undermine nuclear second-strike capabilities directly, but, rather, any technologies that can result in a meaningful shift in the broader balance of power. And the solution is not to preserve second-strike capabilities, but to preserve prevailing power balances more broadly.

When it comes to new technology, this means that the United States should seek to maintain an innovation edge. Washington should also work with other states, including its nuclear-armed rivals, to develop a new set of arms control and nonproliferation agreements and export controls to deny these newer and potentially destabilizing technologies to potentially hostile states.

These are no easy tasks, but the consequences of Washington losing the race for technological superiority to its autocratic challengers just might mean nuclear Armageddon

.

Matthew Kroenig *is Associate Professor of Government and Foreign Service at Georgetown University and Deputy Director for Strategy in the Scowcroft Center for Strategy and Security at the Atlantic Council. His most recent book is* The Logic of American Nuclear Strategy.

Bharath Gopalaswamy is the director of the South Asia Center at the Atlantic Council. He holds a PhD in mechanical engineering with a specialization in numerical acoustics from Trinity College, Dublin.

Indian nuclear forces, 2018

By Hans M. Kristensen and Matt Korda
Source: https://www.tandfonline.com/doi/full/10.1080/00963402.2018.1533162

Nov 01 – India continues to modernize its nuclear arsenal, with at least five new weapon systems now under development to complement or replace existing nuclear-capable aircraft, land-based delivery systems, and sea-based systems. India is estimated to **have produced enough military plutonium for 150 to 200 nuclear warheads, but has likely produced only 130 to 140.** Nonetheless, additional plutonium will be required to produce warheads for missiles now under development, and India is reportedly building several new plutonium production facilities. India's nuclear strategy, which has traditionally focused on Pakistan, now appears to place increased emphasis on China.

Hans Kristensen is the director of the Nuclear Information Project with the Federation of American Scientists (FAS) in Washington, DC. His work focuses on researching and writing about the status of nuclear weapons and the policies that direct them. Kristensen is a co-author to the world nuclear forces overview in the SIPRI Yearbook *(Oxford University Press) and a frequent adviser to the news media on nuclear weapons policy and operations. He has co-authored Nuclear Notebook since 2001.*
Matt Korda is a research associate for the Nuclear Information Project at the Federation of American Scientists. Previously, he worked for the Arms Control, Disarmament, and WMD Non-Proliferation Centre at NATO HQ in Brussels. Korda received his MA in International Peace & Security from the Department of War Studies at King's College London, where he subsequently worked as a research assistant on nuclear deterrence and strategic stability. He also completed an internship with the Verification, Training and Information Centre (VERTIC) in London, where he focused on nuclear security and safeguards. His research interests and recent publications focus on nuclear deterrence, missile proliferation, gender mainstreaming, and alliance management, with regional concentrations on Russia and the Korean Peninsula.

More than 500 'safety events' recorded at UK nuclear submarine base since 2006

Source: https://www.itv.com/news/2018-11-18/more-than-500-nuclear-safety-events-recorded-at-faslane-since-2006/

Nov 18 – **More than 500 safety events have been recorded at the home of the UK's nuclear deterrent since 2006, the Ministry of Defence has revealed.**
Defence Minister Stuart Andrew disclosed the figure in a letter in response to a parliamentary question from Edinburgh SNP MP Deidre Brock.
In total, 505 "events" were recorded over the past 12 years at HM Naval Base Clyde at Faslane, home to most of the UK's nuclear submarine fleet.
In the letter he states: "These events may be near-misses, equipment failures, human error or procedural failings.
"They are raised, however minor they may appear, to encourage a comprehensive, robust reporting culture, undertake learning from experience and to take early corrective action."
There were two Category A incidents listed from 2006 and 2007.
The letter states that Category A events have "actual or high potential for radioactive release to the environment of quantities in excess of IRR99 notification limits".

However, the minister said that in "neither event was any radiological contamination evident".
He continued: "None of the events caused harm to the health of any member of staff on the Naval Base, or to any member of the public."

He said that the MoD takes all incidents, no matter how minor, "extremely seriously" and that they are investigated with appropriate measure put in place.
The figures show an increase in recorded incidents in recent years with 80 in 2016 and 73 last year.
Kate Hudson, CND general secretary, said: "When the MoD took the decision to censor annual nuclear safety reports which had previously been made public, we feared that safety at Faslane was worsening.

"While we welcome a return to a degree of transparency, the figures in the defence minister's letter confirms our fears, revealing a catalogue of accidents in the last three years.
"Many of these incidents involved the Trident submarines which carry Britain's nuclear weapons.
"The incidents add to the dire warnings in September's Public Accounts Committee report which revealed serious infrastructure problems, including huge delays and overspending.

"We hope to see a return to annual reports of the Defence Nuclear Safety Regulator being made available to the public and more transparency in general.
"This information is a requirement in a functioning democracy."
Ms Brock said: "Discovering that there is a succession of safety failures, more than one a week in recent years, really brings home how dangerous Faslane is.
"We've got the world's most dangerous weapons but they seem to be under the control of the Keystone Cops.
"It took six months for the MoD to count up how many incidents there had been, six months to tell me how bad it's been.
"One bad mistake at Faslane could be the end of all of us and it's way past time that those weapons were removed from Scotland.
"We need to see fast action from the MoD to get Faslane back in order. It's only luck that has saved us so far, we can't keep on trusting to it."

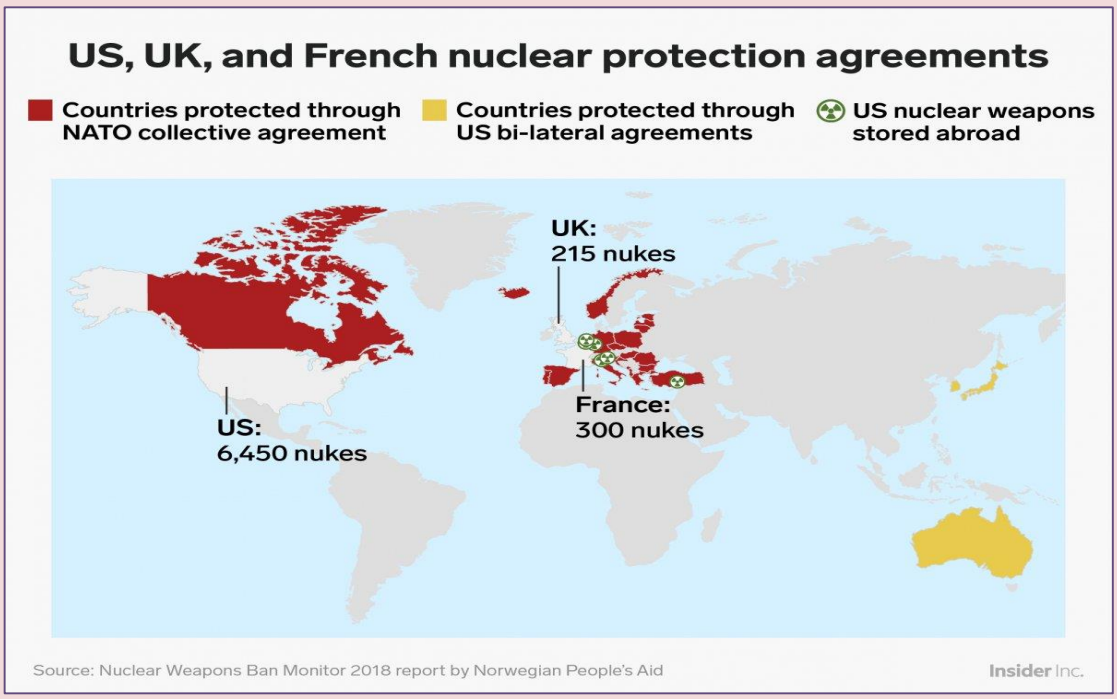
These are the 9 nuclear-armed countries and the 31 allies they have vowed to defend with the world's most devastating weapons

Source: https://www.businessinsider.com.au/these-are-the-9-countries-with-nuclear-weapons-2018-10

Nov 20 – The United Nations has introduced a treaty that it believes will eventually lead to the total elimination of nuclear weapons. A recent watchdog report said the Treaty on the Prohibition of Nuclear Weapons (TPNW) is a historically significant effort that's gaining traction, which highlights the profound

power imbalance between the few nuclear powers and the many countries without the devastating weapons.
"The rate of adherence to the TPNW is faster than for any other weapons-of-mass-destruction (WMD) treaty," the report says.
But with an estimated 14,485 extant nuclear weapons, total elimination is more of a long-term goal.

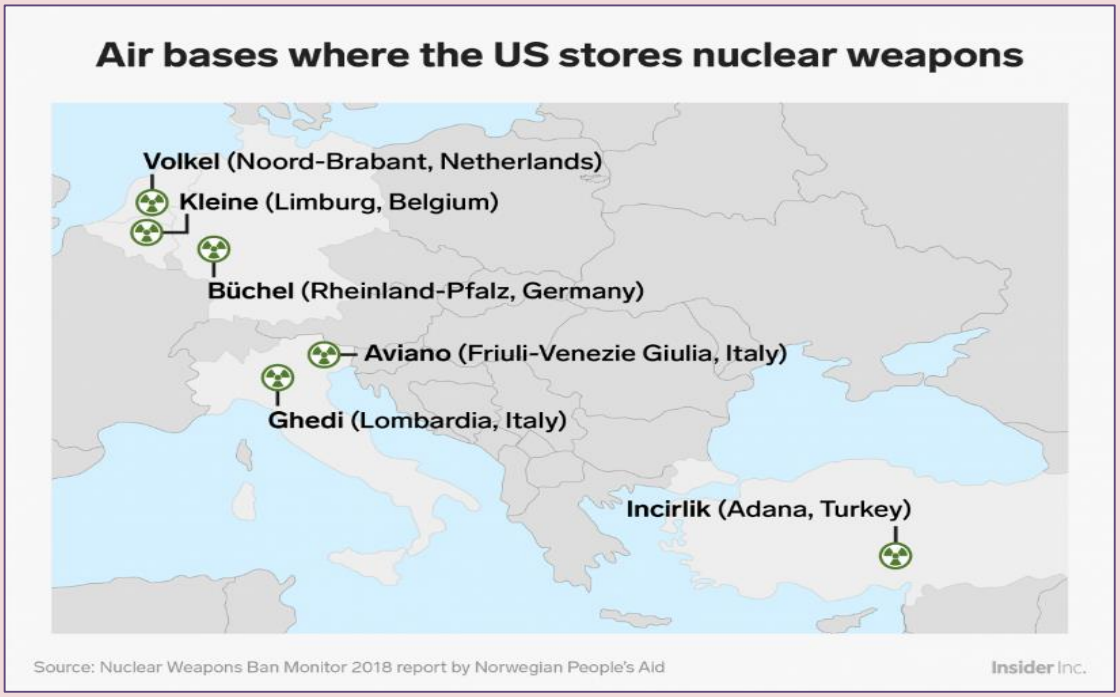
This is an overview of the nine nuclear-armed states and the 31 nuclear-weapon-endorsing states – countries that do not develop or possess nuclear weapons but rely on another nuclear-armed state for protection.



All of these countries would need to make profound changes to reach the UN goal of a nuclear-weapons-free world.

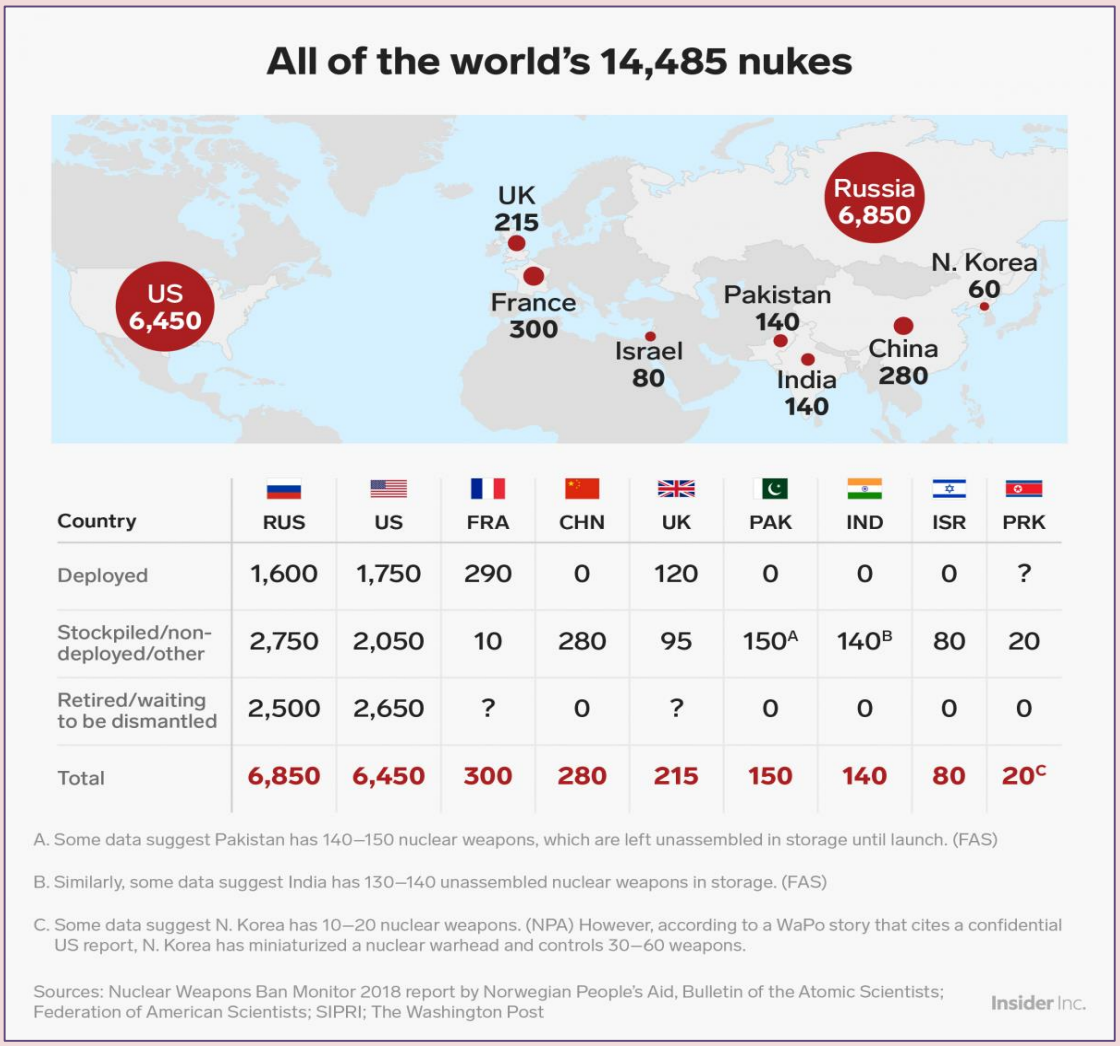
The Russian Federation has an estimated 6,850 nuclear weapons in its arsenal.

Armenia and Belarus, who both rely on Russia's arsenal for "umbrella" protections, stand in violation of TPNW.



A nuclear "triad" refers to a nation's ability to deploy its nuclear arsenal through intercontinental ballistic missiles, sea-launched ballistic missiles, and strategic bombers, as defined by the Nuclear Threat Initiative, an advisory board that conducts research and provides analysis to encourage diplomacy.

The US has agreed to potentially use its nuclear weapons to protect NATO member states, as well as Japan, Australia and South Korea.
Because of these agreements, all 29 NATO member states, and the three who hold bilateral protection agreements with the US, are in violation of TPNW.
The US, which has a nuclear arsenal that's nearly the size of Russia's, is the only nation in the western hemisphere that possesses nuclear weapons, and one of three countries to possess the nuclear "triad."
According to the Nuclear Weapons Ban Monitor, the US is believed to store some 180 nuclear weapons in other countries.
This number has been "significantly reduced since the Cold War," according to the report.
The United Kingdom is a NATO member state and shares in the umbrella protections of the alliance.
The kingdom maintains at least one nuclear-armed submarine on patrol at all times, under a Continuous at Sea Defence Posture, according to NWBM.
British policy also states that the country will not threaten the use of nuclear weapons against any "non-nuclear weapons state."
France, also a NATO member state, can only deliver its nuclear weapons via aircraft and submarines.
The ASMP-A is a 300 kiloton warhead, approximately 20 times the size of the bomb dropped on Hiroshima, Japan, at the end of World War II.



Country	RUS	US	FRA	CHN	UK	PAK	IND	ISR	PRK
Deployed	1,600	1,750	290	0	120	0	0	0	?
Stockpiled/non-deployed/other	2,750	2,050	10	280	95	150[A]	140[B]	80	20
Retired/waiting to be dismantled	2,500	2,650	?	0	?	0	0	0	0
Total	6,850	6,450	300	280	215	150	140	80	20[C]

A. Some data suggest Pakistan has 140–150 nuclear weapons, which are left unassembled in storage until launch. (FAS)

B. Similarly, some data suggest India has 130–140 unassembled nuclear weapons in storage. (FAS)

C. Some data suggest N. Korea has 10–20 nuclear weapons. (NPA) However, according to a WaPo story that cites a confidential US report, N. Korea has miniaturized a nuclear warhead and controls 30–60 weapons.

Sources: Nuclear Weapons Ban Monitor 2018 report by Norwegian People's Aid, Bulletin of the Atomic Scientists; Federation of American Scientists; SIPRI; The Washington Post

Insider Inc.

If a warhead of that size were to drop over Washington, DC, it would result in approximately 280,000 casualties.
China possesses a nuclear "triad," but has agreed not to employ nuclear weapons against any nation in a Nuclear Weapons-Free Zone, which include Latin American and Caribbean nations, as well as some in Africa, the South Pacific and Central Asia.
Although North Korean leader Kim Jong Un has publicly proclaimed a desire to denuclearize the entire Korean peninsula, there is no evidence that he has made any attempt to do so.

Reports vary as to the size of the North Korean nuclear arsenal. While the monitor follows conventional views that the country possesses 10 to 20 nukes, The Washington Post has previously reported that it may hold up to 60, citing confidential US assessments.
Israel has never publicly admitted to possession of nuclear weapons.
Nevertheless, the international community operates on the assumption that since its inception, Israel has developed and maintained a nuclear arsenal.
The size of Israel's cache remains unclear, and though it is possible that the nation holds enough enriched plutonium for 100 to 200 warheads, the NWBM accepts estimates from the Federation of American Scientists, which show that Israel possesses approximately 80 nuclear weapons.

Reuters/ StringerPakistan's Hatf VII (Babur) missile takes off during a test from an undisclosed location in December 2007.

Attempts to develop intercontinental and submarine-launched nuclear missiles indicate that India may soon possess the nuclear "triad."
Mainly due to tensions with Pakistan, some experts have questioned whether India's "no first-use" posture will endure.
Pakistan can deliver its nuclear weapons from the ground and air and is allegedly developing methods of sea-based delivery to complete the nuclear "triad."
Despite facing sanctions, Pakistan is reportedly expanding its nuclear arsenal faster than any other nation.
Similar to British policy, Pakistan claims it will not use or threaten to use its nuclear arsenal against any "non-nuclear" state, leaving many questions unanswered on the potential use against neighbour India, which also maintains nuclear weapons.


ICI International
CBRNE INSTITUTE
CBRNE-Terrorism Newsletter
W O M D
C2BRNE DIARY
EXPLOSIVE NEWS

Explosives sent to Obama, Clinton, and CNN: All about the pipe bombs and their packaging

Source: http://dbpost.com/explosives-sent-to-obama-clinton-and-cnn-all-about-the-pipe-bombs-and-their-packaging/

Oct 25 – The New York Police on Wednesday obstructed the further ongoing of the suspicious package of potential explosive containing a pipe bomb, which was being sent to former US President Barack Obama, former US presidential candidate Hillary Clinton and other high profile Democrats.

The explosive was taken in custody by the New York police and no casualties has been transpired, while New York officials described it as "an act of terrorism".

NY Police Department's Deputy Commissioner of Intelligence & Counterterrorism John Miller said the devices in the packages appear to be pipe bombs.

"This clearly is an act of terror attempting to undermine our free press and leaders of this country through acts of violence," New York Mayor Bill de Blasio told a news conference.

CNN news bureau in New York at the Time Warner Centre also received suspicious explosives packets similar to those sent to Obama and Clinton containing a white powder inside, addressed to John Brennan, former Director Central Intelligence Agency.

NY Police Department's Deputy Commissioner of Intelligence & Counterterrorism John Miller said the devices in the packages appear to be pipe bombs.

Jim Sciutto, co-anchor of CNN Newsroom & Chief National Security Correspondent stated that Explosive devices sent to Obama, Clinton, CNN & others appear to have sulphur substance; FBI counterterrorism team now leading an investigation.

A similar pipe bomb was delivered earlier this week to the home of George Soros, a major Democratic Party donor.

CNN statement

CNN Worldwide President, Jeff Zucker said, "There is a total and complete lack of understanding at the White House about the seriousness of their continued attacks on the media," CNN Worldwide President Jeff Zucker said in a statement Wednesday afternoon. "The President, and especially the White House Press Secretary, should understand their words matter. Thus far, they have shown no comprehension of that," he added.

Details about explosives sent to Obama, Clinton and other Democrats

Barack Obama

- On Wednesday morning in routine mail screening, a suspicious package containing explosives was found.

- The package was in a manilla envelope and had multiple stamps on it. It appeared to be a working explosive, although analysis is pending further testing.
- The package listed a return address as one belonging to Debbie Wasserman Schultz

Hillary Clinton

- Secret Service screeners reviewing mail to Hillary Clinton at an outside mail sorting facility find a potentially explosive device addressed to the former secretary of state.
- The package was in a manilla envelope and had multiple stamps on it. It appeared to be a working explosive, although analysis is pending further testing.
- The package listed a return address as one belonging to Debbie Wasserman Schultz.

CNN/Brennan

- A suspicious parcel with a manila outer packaging and stamps, is discovered in CNN Bureau at the Time Warner Centre Wednesday, addressed to former CIA director John Brennan.
- The device inside the package appeared to be a "live explosive," NYPD commissioner O'Neill said.
- An envelope with white powder was also found in the packaging.
- The device also included a parody image of the ISIS flag.
- The building was evacuated while the package is removed.

Suspicious packages were also sent to Debbie Wasserman Schultz, George Soros, Eric Holder, and Maxine Waters, all those prominent figures were also the targets of explosive devices.

All the devices were packed in envelopes lined with Bubble Wrap and bearing return addresses with the name of Debbie Wasserman Schultz, the Florida congresswoman who was once chairwoman of the Democratic National Committee, the F.B.I. said. The mailing labels were computer-printed, and six first-class stamps were affixed to all of the envelopes.

Over the past three days, at least seven explosive devices have been discovered.

UPDATE (Oct 26+28): US police are investigating a twelfth suspicious package after pipe bombs were sent to prominent critics of Donald Trump.One of the parcels was addressed to the Democrat senator Cory Booker in Florida, with the FBI saying it is similar in appearance to the others that have been seized. Another was addressed to the former director of national intelligence, James Clapper, care of CNN. Mr Clapper told the news channel, where he works as an analyst, that the incidents were "serious" and "definitely domestic terrorism". Another parcel bomb posted to CNN (#12).

Europol conference in Portugal on improvised explosive devices and radiological materials

Source: https://www.europol.europa.eu/newsroom/news/europol-conference-in-portugal-improvised-explosive-devices-and-radiological-materials

Oct 26 – CEPOL and Europol, supported by the Portuguese Guarda Nacional Republicana (GNR) organised a conference and training session attended by 75 CBRN and/or explosives experts of the European Explosive Ordnance Disposal Network (EEODN), which took place from 16th to 19th of October 2018, at the School of Guard, at Queluz, Portugal.

Officers from 26 EU Member States plus Norway and the United States, together with experts from specialised agencies such as the EU DG Migration and

Home Affairs, the Joint Research Centre – Geel, the NATO – C-IED CoE Madrid - Spain, the NATO EOD CoE Trencin – Slovakia, INTERPOL, the Organisation for the Prohibition of Chemical Weapons (OPCW), the International Atomic Energy Agency (IAEA) and the Europol - CBRN & Explosives team were present.
The main purpose of the conference was to promote the debate on recent cases involving the use of improvised explosive devices (IEDs) and radiological materials (CBRN). The 23 experts involved as trainers were able to develop the participants' knowledge, skills, techniques and tools through the analysis of the most recent incidents occurring in Europe.
This joint CEPOL - Europol activity happened for the first time in Portugal, and the training programme was designed and jointly prepared by the National Republican Guard and Europol.
The participants were invited to combine all their knowledge and "hands on" capacity, challenged by the possibility of using innovative strategies and techniques for the neutralisation of the highly complex and dangerous threats.
The Conference ended on 19th October, after a debriefing on the methodologies, strategies and techniques used during the training, aiming to provide a reflection on the best practices to face this kind of threats.

How police use a 'total containment vessel' to haul away explosive devices

Source: https://www.theverge.com/2018/10/24/18019236/pipe-bomb-removal-nypd-nyc-obama-clinton-cnn

Oct 24 – On Wednesday, explosive devices were sent to CNN headquarters at the Time Warner Center in Manhattan. Bombs were also sent to former President Barack Obama and former Secretary of State Hillary Clinton, in what New York City Mayor Bill de Blasio is calling "an act of terror." This spate of would-be bombings have cast light on a little-known device used by police to haul away the explosive material called a "total containment vessel," or TCV.
The TCV is designed to absorb the blast from a bomb. It's been described as "an inside-out diving vessel." In 2016, after a pressure-cooker bomb went off in Manhattan, police gave reporters a tour of the high-tech device.
"Instead of keeping the pressure out and keeping you alive in five fathoms of water, it keeps the pressure in," [Lt. Mark Torre, the commanding officer of the NYPD's bomb squad] explained. Should a bomb explode inside, tiny vents allow pressure to escape. "It sounds like a hammer hitting a piece of steel," he said.
The NYPD has three TCVs located throughout the five boroughs to be deployed at a moment's notice, counterterrorism Chief James Waters told the *Daily News* in 2016. Inside

the chamber is a "basket" where the explosive rests to prevent explosion-triggering turbulence during the drive.

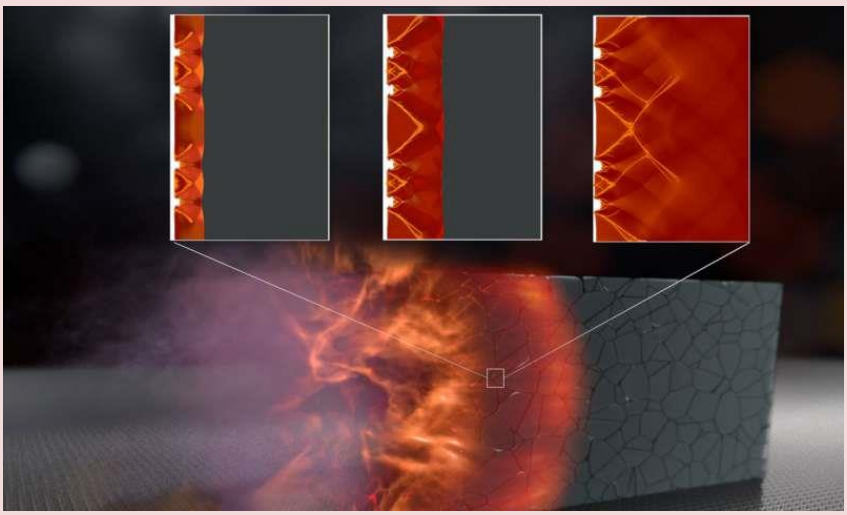
Such vessels are often capable of containing a blast of 25 pounds of TNT or more, and they are increasingly a common piece of equipment for police agencies across the country.

Images of the spherical TCV are now making the rounds on Twitter, with local news helicopters even tracking it as its hauled north to Rodman's Neck, a peninsula in the Bronx where police destroy unexploded bombs.

Uncovering secret structure to safer explosives

Source: https://phys.org/news/2018-10-uncovering-secret-safer-explosives.html#jCp

Oct 18 – A team of scientists at Lawrence Livermore National Laboratory (LLNL) has shown that the structure of microscopic pores in high explosive materials can significantly impact performance and safety. These findings — published recently as the cover article in the journal *Propellants, Explosives, Pyrotechnics* — open the door to the possibility of tuning high explosives by engineering their microstructure.



Supercomputer simulations of shock-induced explosive reactions suggest that the microstructure of heterogeneous solid explosive materials impact performance and safety. Credit: Lawrence Livermore National Laboratory

"The funny thing about explosives is that they have these little defects and pores and holes," said research scientist Keo Springer, lead author on the paper and researcher at LLNL's High Explosives Applications Facility. "It turns out that that's an important part of what makes them work. Explosive performance, in a broad sense, isn't just a chemistry question, it's a microstructure question."

In most high explosives, detonation is initiated through a process where pores get compressed by a shockwave. When a pore collapses, it creates a hotspot capable of

initiating a chemical reaction in the microscopic crystalline grains of explosive material. This research focused on an explosive compound called HMX, which is known to be more sensitive and more dangerous to work with than other explosives. The fundamental question at the root of this study was whether it makes a difference if the pores are located in the interior of the grains or on their surface.

"We found out that when pores are at the surface, they speed up the reaction," Springer said. "We also discovered that if a shockwave hits a number of surface pores at once, they bootstrap each other. It's an explosive party, and they party well together."

In addition to pore location, the team examined whether it makes a difference if the porosity is distributed across many small pores or across fewer larger pores. While they showed that many small pores can work together to accelerate one another's burning, they also were able to identify a threshold where pores become so small that the reaction is extinguished.

This examination was conducted in a series of numerical simulations on LLNL supercomputers with the multi-physics code, ALE3D. Next steps for the research team—Springer, along with LLNL scientists Sorin Bastea, Al Nichols, Craig Tarver and Jack Reaugh—include verifying that the numerical simulations capture the real physical and chemical processes. A direct way to do that is to conduct micro-scale experiments to quantify pore collapse mechanisms and reactivity.

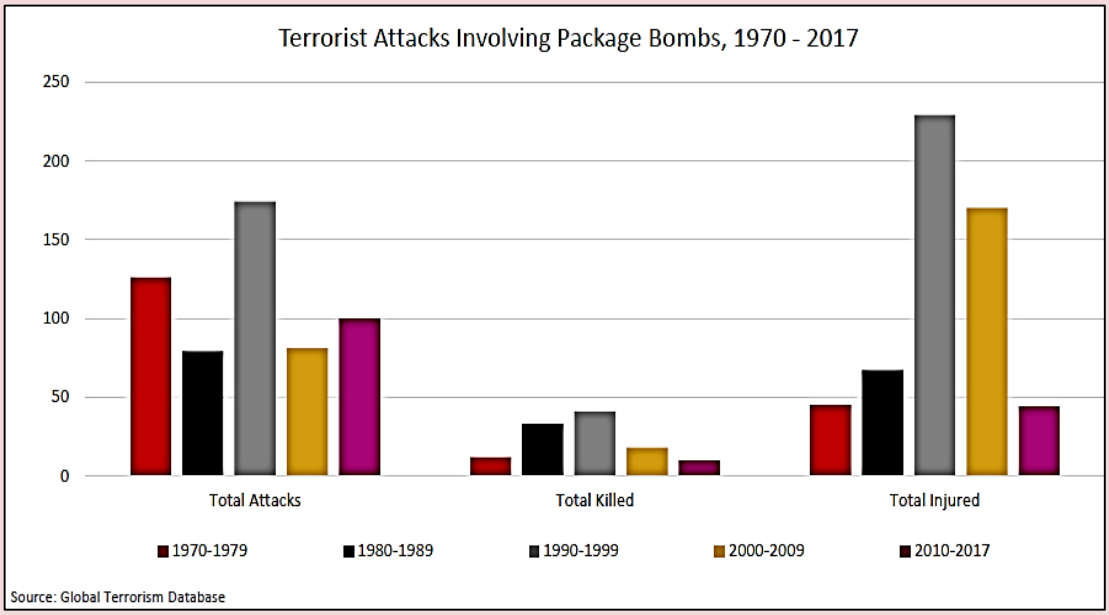
"Validation is the tough part," Springer said. "Ideally, we would need a really good magnifying glass and the ability to stop time. We're talking about sub-micron resolution with a shutter speed on the order of nanoseconds. What's neat is that the research community is starting to work on this.

"If we can engineer initiation properties into the microstructure of explosives, it would be a game changer for industry and for the safety of the nuclear stockpile. But we have a long way to go to realize that vision. This type of research is very important, but just one of the first steps."

More information: *H. Keo Springer et al. Modeling The Effects of Shock Pressure and Pore Morphology on Hot Spot Mechanisms in HMX, Propellants, Explosives, Pyrotechnics (2018). DOI: 10.1002/prep.201800082*

Terrorist Attacks Involving Package Bombs, 1970 — 2017

Source: https://www.start.umd.edu/pubs/START_PackageBombs_FactSheet_Oct2018.pdf



Between 1970 and 2017, 560 terrorist attacks involved explosives in letters, parcels, or packages sent in the mail or made to appear as if they were sent in the mail.

Terrorist attacks involving package bombs were least likely to be successful compared to attacks involving other types of weapons, with explosives detonating in 39 percent of all package bomb attacks. In comparison, 55 percent of pipe bomb attacks (excluding those

sent in packages) were successful. Overall, 89 percent of all terrorist attacks worldwide during this period were successful, regardless of weapons used.

Between 1970 and 2017, there were 39 terrorist attacks involving other dangerous substances sent through the mail.
● Thirty-six of these attacks occurred between 2000 and 2017.
● The materials used in these attacks include anthrax (21 attacks), ricin (6), 1080 pesticide (4), and cyanide (3). In five cases the specific type of material was not identified.
● The majority of these attacks occurred in the United States (23). Other locations included New Zealand (6), Kenya (3), Czech Republic (2), Pakistan (2), the United Kingdom (2), and Chile (1).

▶▶ Read the full paper at source's URL.

ISIS Still Has Combat Drone Capabilities

Source: https://i-hls.com/archives/86595

Nov 09 – A recent publication by the Meir Amit Intelligence and Terrorism Information Center evaluates that ISIS still has drone warfare capabilities despite setbacks and Syria and Iraq. The drones might be used against Western targets overseas.

According to the report, during the years in which it was active in Syria and Iraq, ISIS made extensive use of drones, both for offensive and defensive purposes. It handled the drones to carry out attacks ("explosive drones"), to collect intelligence, and even for propaganda purposes (documenting attacks by suicide bombers in order to disseminate the photos through ISIS's media foundations). Upon the collapse of the Islamic State and in view of the heavy pressure exerted on ISIS on the various fronts, the organization's capability of handling drones, which ISIS had developed in Syria and Iraq since 2014, sustained a significant blow.

However, it seems that ISIS still possesses a certain amount of drones. Furthermore, in Denmark, the authorities recently detained two men who apparently were part of an ISIS network for purchasing drones in Europe. Their detention indicates that ISIS is still making efforts to purchase drones and deliver them to its operatives in Syria (and maybe even in Iraq).

A potential threat is handling drones for terror attacks by ISIS operatives or supporters abroad. Drones used for civilian purposes are sold on the open market and can be easily bought, at affordable prices.

Recently, a media foundation affiliated with ISIS released a threatening poster showing the Eiffel Tower with a drone with a large canister (possibly intended for a weapon) beside it. The poster had an English inscription, "Await for our surprises."

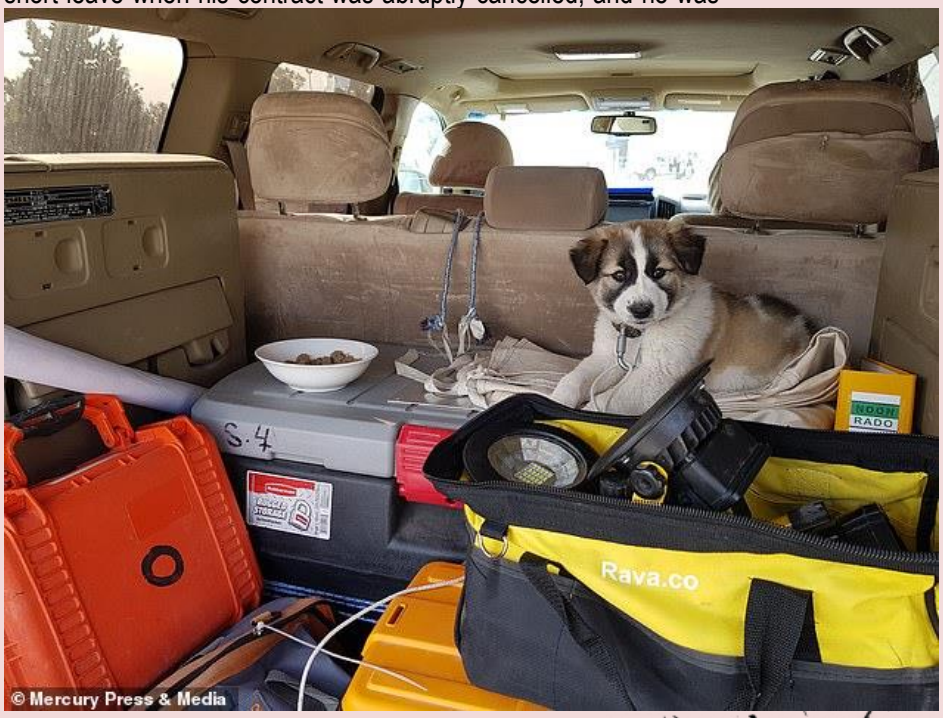
In February 2018, ISIS also released a poster threatening to operate an offensive model airplane against a Western city. In the ITIC's assessment, ISIS supporters abroad have the ability to realize such threats by purchasing civilian drones and operating them as offensive weapons against people, facilities of symbolic importance, or other pinpoint targets.07

The dog who saved me from horrors of war: British bomb disposal expert has emotional reunion with puppy he plucked from rubble of bombed-out school in Syria

Source: https://www.dailymail.co.uk/news/article-6362501/Former-soldier-reunited-abandoned-dog-Barrie-saved-rubble-shattered-Syria.html

Nov 07 – Sean, who now runs a gym, said: 'I think as soon as Barrie and I bonded, where I could pick her up, for me she'd already become my dog.
'When we got back to camp, she lived in my room, I looked after her, I was responsible for her. She slept in my room, I was training her, I was feeding her.

'She stayed with me every day all day. She did jobs with me, I'd wake up, she'd come eat with me, she'd then sit in the passenger seat of my car when we drove to Raqqa.'
Sean contacted War Paws - a charity based in Iraq who specialise in bringing dogs home from war-torn areas - to find a way to bring Barrie back with him after his contract was due to run out.
In February, Sean set up a gofundme page to bring Barrie to the UK and raised £4,500 - but that was the first of many hurdles in their path.
Barrie was brought to Iraq in April where she was vaccinated and checked by War Paws before being flown to Jordan in August, where she was quarantined for two months.
In April, after four months in Syria, Sean returned to the UK for a short leave when his contract was abruptly cancelled, and he was informed that he wouldn't be returning to Syria.



He said: 'I might be one of the only people who was unhappy not to go back to Syria. I was on the way to the airport with my dad when I got a message telling me not to board my flight and go home.
'I thought there might be a security issue, but then I got a call that night saying the contract is cancelled and that everyone is being sent back home.
'I put the phone down and immediately called the charity, I didn't think of anything else and tried to see how I could get Barrie home.

'When it came to going home without her, I thought I'd never be able to leave her so I started thinking about how I could bring her back.

'It's very difficult to be apart, my biggest issue was that I never had that moment with her to say goodbye as when I left I thought I'd see her in a couple weeks.

'But then months passed and she's gone from a puppy to a full-grown dog. That was hard for me, as I worried she was a totally different dog.'

The plan to fly Barrie to London Heathrow in late October quickly collapsed as Barrie was missing some paperwork and the nervous pooch wasn't allowed to travel.

Sean was prepared to fly to Jordan to pick up his best friend, but owner of War Paws, Louise Hastie, came to the rescue as she was already flying two dogs from Jordan to Paris.

Sean made the 12-hour journey from Essex to Paris at 6am on Saturday, November 3, in what he says was a surreal feeling.

Sean said: 'All the help we've received to bring us together has been amazing, just to bring one dog to Essex, it's been incredible.

'Thinking about having Barrie with me now, the life we can have together - it's surreal.

'One of my biggest fears was that she wouldn't recognise who I was, or that she would be a different dog to the girl I left.

'It was pure joy when she realised who I was. She's exactly as she was back in Syria, it was just great to have my dog again.

'I'd be willing to travel across the whole world to have Barrie with me.'

New High-Frequency Technology Can Detect Mail Bombs

Source: https://i-hls.com/archives/86800

Nov 16 – Screening inbound mail against postal IEDs and other personal harm devices is becoming a standard practice in organizations. The past series of mail bombs sent to President Barack Obama, Vice President Joe Biden, Hillary Clinton and others have put a spotlight on the security of mailing and delivery services.

The T-SENSE, an all-in-one sensor solution designed to improve the security and safety of postal facilities around the world, was unveiled by HUBNER.

Us ing high-frequency technology, T-SENSE detects concealed objects, powders and hazardous substances in packages. Leveraging terahertz waves, T-SENSE penetrates paper, clothing, plastic and many other materials in just seconds, similar to airport screening machines.

"Every post office or mail room in the world represents a gateway for dangerous attacks and must be closely protected," said Thorsten Sprenger, Head of Terahertz-Technology & Photonics at HÜBNER. "T-SENSE effectively detects potential hazards while also reducing costly false alarms. It is also safe for security employees, with no harmful radiation omitted during operation, unlike traditional security solutions, such as x-rays."

The new T-SENSE can scan letters and packages up to a thickness of 5 centimeters. The turnkey system includes a plug-and-play setup and intuitive user interface. The compact, stand-alone device includes an integrated computer with corresponding software as well as a touch-screen monitor, mouse and keyboard, according to prnewswire.com.

ICI International CBRNE INSTITUTE

CBRNE-Terrorism Newsletter

C²BRNE DIARY

CYBER NEWS

Safeguarding the U.S. energy infrastructure

Source: http://www.homelandsecuritynewswire.com/dr20181030-safeguarding-the-u-s-energy-infrastructure

Oct 30 – Nearly every aspect of our daily lives — from shopping for groceries through a smartphone app to keeping up with friends and family on social media, or relying on smart grid technology to power homes and businesses – is connected to the vast world of the internet. Because of this, it might seem as if there's nothing we can do to protect ourselves from a cyberattack, but according to the U.S. Department of Energy's Office of Cybersecurity, Energy Security, and Emergency Response, "Everyone has a role in making cyberspace secure."

That sense of shared responsibility is not only this year's overarching theme for National Cybersecurity Awareness Month, but it has also inspired the work of many scientists, including cybersecurity expert Sean Peisert of the DOE's Lawrence Berkeley National Laboratory (Berkeley Lab).

Peisert is one of thousands of DOE scientists who have dedicated their careers to finding the best solutions to some of our nation's biggest problems. He is a staff scientist in Berkeley Lab's Computational Research Division, an associate adjunct professor of computer science at UC Davis, and the chief scientist for cybersecurity for CENIC (Corporation for Education Network Initiatives in California).

In recognition of National Cybersecurity Awareness Month – an annual initiative first launched in October 2004 by the Department of Homeland Security and the National Cyber Security Alliance to raise awareness about the importance of staying safe and secure online – Peisert discussed with LBL's Theresa Duque new cybersecurity approaches that have the potential to keep our energy infrastructure safe.

Theresa Duque: What can we do to protect energy infrastructure equipment connected to the internet?

Sean Peisert: Even though computer systems are complex, the network-connected physical components that operate the power grid – such as the transformers, tap changers, and power inverters, for example – have characteristics about their operation that may make cybersecurity more tractable.

Specifically, these physical components obey the laws of physics. Therefore, we have shown that it is possible to measure – through insights about those laws, the use of proper sensors, and statistical algorithms – whether they're performing the way they were designed to behave before a cyberattack or a weather-related event, then watch for changes, and determine the cause.

This notion that we can determine if a system that controls power grid equipment is obeying the laws of physics is a very different approach to detecting cyberattacks against more "traditional" computing targets where there is no such set of physical laws that the systems must obey.

Duque: What are the most promising new approaches for keeping our power grids and aging energy infrastructures safe?

Peisert: I think one of the most promising approaches lies in marrying "safety engineering" principles – which are grounded in the immutable laws of physics – with computer security. For example, at Berkeley Lab, I am currently leading a project with several academic and industry partners to develop acyberthreat detection application that would send an early warning to grid operators if equipment like a capacitor bank switch or transformer tap changer in a substation, for example, is behaving in an unexpected way due to a cyberattack, long before existing techniques would detect such behavior, and before the behavior could result in actual grid instability.

For this project, we are leveraging distribution-level phasor measurement units to detect cyber-physical attacks on the power distribution grid to capture information about the distribution grid's physical state. We then combine this data with SCADA (supervisory control and data acquisition) information, which is commonly used in electric grid monitoring, to provide real-time feedback about system performance.

Our use of high-frequency power sensors provides a redundant set of measurements that gives us a high-fidelity way of tracking what is going on in the power distribution grid. By looking at those measurements alone, or by looking for discrepancies by comparing those measurements with what was reported by the equipment, we can have better insight into whether a hacker was trying to manipulate those components in the power distribution grid.

In a separate project, we are also applying related techniques to detecting and mitigating attacks on rooftop solar inverters to maintain grid stability in the face of such attacks.

New techniques expose your browsing history to attackers

Source: http://www.homelandsecuritynewswire.com/dr20181030-new-techniques-expose-your-browsing-history-to-attackers

Oct 30 – Security researchers at UC San Diego and Stanford have discovered four new ways to expose Internet users' browsing histories. These techniques could be used by hackers to learn which websites users have visited as they surf the web.

The techniques fall into the category of "history sniffing" attacks, a concept dating back to the early 2000s. But the attacks demonstrated by the researchers at the 2018 USENIX Workshop on Offensive Technologies (WOOT) in Baltimore can profile or 'fingerprint' a user's online activity in a matter of seconds, and work across recent versions of major web browsers.

UCSD notes that all of the attacks the researchers developed in their WOOT 2018 paper worked on Google Chrome. Two of the attacks also worked on a range of other browsers, from Mozilla Firefox to Microsoft Edge, as well various security-focused research browsers. The only browser which proved immune to all of the attacks is the Tor Browser, which doesn't keep a record of browsing history in the first place.

"My hope is that the severity of some of our published attacks will push browser vendors to revisit how they handle history data, and I'm happy to see folks from Mozilla, Google, and the broader World Wide Web Consortium (W3C) community already engage in this," said Deian Stefan, an assistant professor in computer science at the Jacobs School of Engineering at UC San Diego and the paper's senior author.

"History sniffing": smelling out your trail across the web

Most Internet users are by now familiar with "phishing;" cyber-criminals build fake websites which mimic, say, banks, to trick them into entering their login details. The more the phisher can learn about their potential victim, the more likely the con is to succeed. For example, a Chase customer is much more likely to be fooled when presented with a fake Chase login page than if the phisher pretends to be Bank of America.

After conducting an effective history sniffing attack, a criminal could carry out a smart phishing scheme, which automatically matches each victim to a faked page corresponding to their actual bank. The phisher preloads the attack code with their list of target banking websites, and conceals it in, for example, an ordinary-looking advertisement. When a victim navigates to a page containing the attack, the code runs through this list, testing or 'sniffing' the victim's browser for signs that it's been used to visit each target site. When one of these sites tests positive, the phisher could then redirect their victim to the corresponding faked version.

The faster the attack, the longer the list of target sites an attacker can 'sniff' in a reasonable amount of time. The fastest history sniffing attacks have reached rates of thousands of URLs tested per second, allowing attackers to quickly put together detailed profiles of web surfers' online activity. Criminals could put this sensitive data to work in a number of ways besides phishing: for example, by blackmailing users with embarrassing or compromising details of their browsing histories.

History sniffing can also be deployed by legitimate, yet unscrupulous, companies, for purposes like marketing and advertising. A 2010 study from UC San Diego documented widespread commercial abuse of previously known history sniffing attack techniques, before these were subsequently fixed by browser vendors.

"You had internet marketing firms popping up, hawking pre-packaged, commercial history sniffing 'solutions', positioned as analytics tools," said Michael Smith, a computer science Ph.D. student at UC San Diego and the paper's lead author. The tools purported to offer insights into the activity of their clients' customers on competitors' websites, as well as detailed profiling information for ad targeting—but at the expense of those customers' privacy.

"Though we don't believe this is happening now, similar spying tools could be built today by

abusing the flaws we discovered," said Smith.

New attacks

The attacks the researchers developed, in the form of JavaScript code, cause web browsers to behave differently based on whether a website had been visited or not. The code can observe these differences—for example, the time an operation takes to execute or the way a certain graphic element is handled—to collect the computer's browsing history. To design the attacks, researchers exploited features that allow programmers to customize the appearance of their web page—controlling fonts, colors, backgrounds, and so forth—using Cascading Style Sheets (CSS), as well as a cache meant to improve to performance of web code.

The researchers' four attacks target flaws in relatively new browser features. For example, one attack takes advantage of a feature added to Chrome in 2017, dubbed the "CSS Paint API", which lets web pages provide custom code for drawing parts of their visual appearance. Using this feature, the attack measures when Chrome re-renders a picture linked to a particular target website URL, in a way invisible to the user. When a re-render is detected, it indicates that the user has previously visited the target URL. "This attack would let an attacker check around 6,000 URLs a second and develop a profile of a user's browsing habits at an alarming rate," said Fraser Brown, a Ph.D. student at Stanford, who worked closely with Smith.

Though Google immediately patched this flaw—the most egregious of the attacks that the researchers developed—the computer scientists describe three other attacks in their WOOT 2018 paper that, put together, work not only on Chrome but Firefox, Edge, Internet Explorer, but on Brave as well. The Tor Browser is the only browser known to be totally immune to all the attacks, as it intentionally avoids storing any information about a user's browsing history.

As new browsers add new features, these kinds of attacks on privacy are bound to resurface.

A proposed defense

The researchers propose a bold fix to these issues: they believe browsers should set explicit boundaries controlling how users' browsing histories are used to display web pages from different sites. One major source of information leakage was the mechanism which colors links either blue or purple depending on whether the user has visited their destination pages, so that, for example, someone clicking down a Google search results page can keep their place. Under the researchers' model, clicking links on one website (e.g., Google) wouldn't affect the color of links appearing on another website (e.g., Facebook). Users could potentially grant exceptions to certain websites of their choosing. The researchers are prototyping this fix and evaluating the trade-offs of such a privacy-conscious browser.

New Device Challenges Terrorists

Source: https://i-hls.com/archives/86414

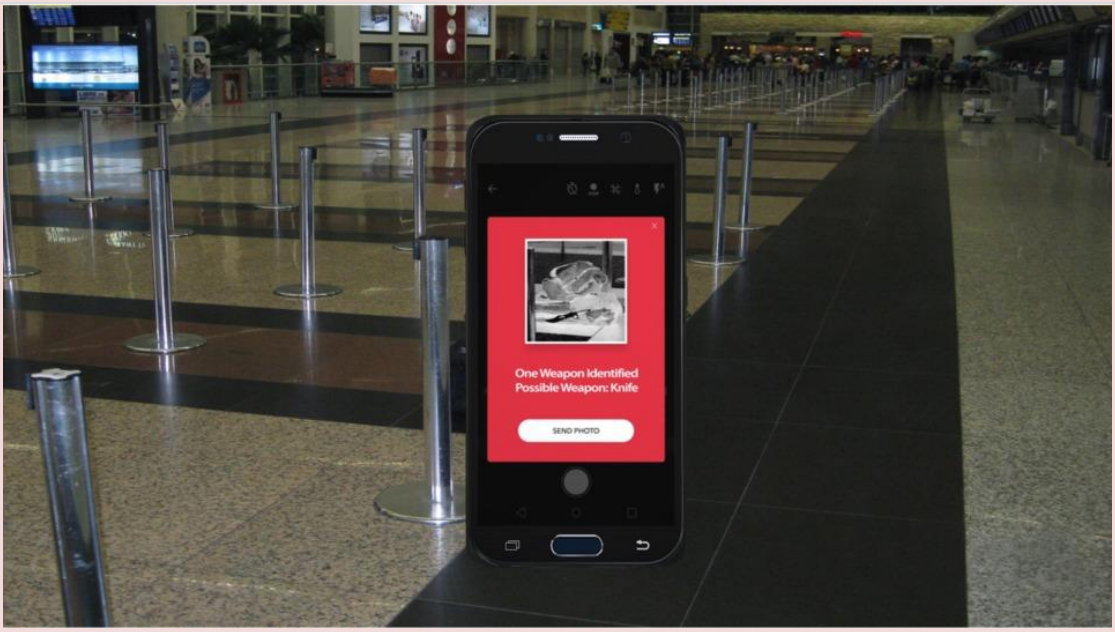
Oct 30 – Asymmetric warfare, meaning conventional militaries combatting guerrilla and terrorist organizations, has long posed a challenge for states. New technology combining mobile platforms with the Internet of Things (IoT) and artificial intelligence (AI) into a single product called SWORD, able to identify, manage and mitigate immediate threats.

SWORD features an integrated, infrared-object-detection HD camera and proprietary algorithms paired with the company's facial recognition software, and all placed in what appears to be a regular case for an iPhone or iPad. It can detect weapons from a distance, and inform its user whether an approaching individual is armed.

Royal Holdings Technologies Corp. stands behind SWORD technology. Essentially, SWORD allows undercover security personnel to mingle with crowds, holding up their devices from between 10 meters to 30 meters away.

SWORD has no "pause and pose" requirement. Scanning takes less than 1.5 seconds, and clothing doesn't need to be removed.

Additionally, SWORD doesn't need to be plugged in and has a battery life of up to 8 hours on the iPhone 8 or iPad Pro, and devices can also be mounted on tripods to create random screening points.



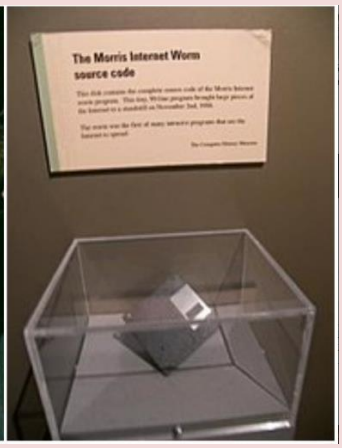
If an object is detected or person of interest is identified, the operator is immediately alerted.
SWORD detects both metallic and non-metallic threats that have been concealed on an individual, including a wide range of weapons, explosive devices, tactical surveillance counter-measures (TCSM) and even 3D-printed weapons.
AI machine learning allows the system to constantly add new faces and threats in near real-time to ensure defense intelligence is always up to date, as reported in americansecuritytoday.com.

30 years ago, the world's first cyberattack set the stage for modern cybersecurity challenges

By Scott Shackelford

Source: http://www.homelandsecuritynewswire.com/dr20181106-30-years-ago-the-world-s-first-cyberattack-set-the-stage-for-modern-cybersecurity-challenges

Nov 06 – Back in November 1988, Robert Tappan Morris, son of the famous cryptographer Robert Morris Sr., was a 20-something graduate student at Cornell who wanted to know how big the internet was – that is, how many devices were connected to it. So he wrote a program that would travel from computer to computer and ask each machine to send a signal back to a control server, which would keep count.



The program worked well – too well, in fact. Morris had known that if it traveled too fast there might be problems, but the limits he built in weren't enough to keep the program from clogging up large sections of the internet, both copying itself to new machines and sending those pings back. When he realized what was happening, even his messages warning system administrators about the problem couldn't get through.

His program became the first of a particular type of cyber attack called distributed denial of service," in which large numbers of internet-connected devices, including computers, webcams and other smart gadgets, are told to send lots of traffic to one particular address, overloading it with so much activity that either the system shuts down or its network connections are completely blocked.

As the chair of the integrated Indiana University Cybersecurity Program, I can report that these kinds of attacks are increasingly frequent today. In many ways, Morris's program, known to history as the "Morris worm," set the stage for the crucial, and potentially

devastating, vulnerabilities in what I and others have called the coming "Internet of Everything."

Unpacking the Morris worm

Worms and viruses are similar, but different in one key way: A virus needs an external command, from a user or a hacker, to run its program. A worm, by contrast, hits the ground running all on its own. For example, even if you never open your email program, a worm that gets onto your computer might email a copy of itself to everyone in your address book.

In an era when few people were concerned about malicious software and nobody had protective software installed, the Morris worm spread quickly. It took 72 hours for researchers at Purdue and Berkeley to halt the worm. In that time, it infected tens of thousands of systems – about 10 percent of the computers then on the internet. Cleaning up the infection cost hundreds or thousands of dollars for each affected machine.

In the clamor of media attention about this first event of its kind, confusion was rampant. Some reporters even asked whether people could catch the computer infection. Sadly, many journalists as a whole haven't gotten much more knowledgeable on the topic in the intervening decades.

Morris wasn't trying to destroy the internet, but the worm's widespread effects resulted in him being prosecuted under the then-new Computer Fraud and Abuse Act. He was sentenced to three years of probation and a roughly US$10,000 fine. In the late 1990s, though, he became a dot-com millionaire – and is now a professor at MIT.

Rising threats

The internet remains subject to much more frequent – and more crippling – DDoS attacks. With more than 20 billion devices of all types, from refrigerators and cars to fitness trackers, connected to the internet, and millions more being connected weekly, the number of security flaws and vulnerabilities is exploding.

In October 2016, a DDoS attack using thousands of hijacked webcams – often used for security or baby monitors – shut down access to a number of important internet services along the eastern U.S. seaboard. That event was the culmination of a series of increasingly damaging attacks using a botnet, or a network of compromised devices, which was controlled by software called Mirai. Today's internet is much larger, but not much more secure, than the internet of 1988.

Some things have actually gotten worse. Figuring out who is behind particular attacks is not as easy as waiting for that person to get worried and send out apology notes and warnings, as Morris did in 1988. In some cases – the ones big enough to merit full investigations – it's possible to identify the culprits. A trio of college students was ultimately found to have created Mirai to gain advantages when playing the "Minecraft" computer game.

Fighting DDoS attacks

But technological tools are not enough, and neither are laws and regulations about online activity – including the law under which Morris was charged. The dozens of state and federal cybercrime statutes on the books have not yet seemed to reduce the overall number or severity of attacks, in part because of the global nature of the problem.

There are some efforts underway in Congress to allow attack victims in some cases to engage in active defense measures – a notion that comes with a number of downsides, including the risk of escalation – and to require better security for internet-connected devices. But passage is far from assured.

There is cause for hope, though. In the wake of the Morris worm, Carnegie Mellon University established the world's first Cyber Emergency Response Team, which has been replicated in the federal government and around the world. Some policymakers are talking about establishing a national cybersecurity safety board, to investigate digital weaknesses and issue recommendations, much as the National Transportation Safety Board does with airplane disasters.

More organizations are also taking preventative action, adopting best practices in cybersecurity as they build their systems, rather than waiting for a problem to happen and trying to clean up afterward. If more organizations considered cybersecurity as an important element of corporate social responsibility, they – and their staff, customers and business partners – would be safer.

In "3001: The Final Odyssey," science fiction author Arthur C. Clarke envisioned a future where humanity sealed the worst of its weapons in a vault on the moon – which included room for the most malignant computer viruses ever created. Before the next iteration of the Morris worm or Mirai does untold damage to the modern information society, it is up to

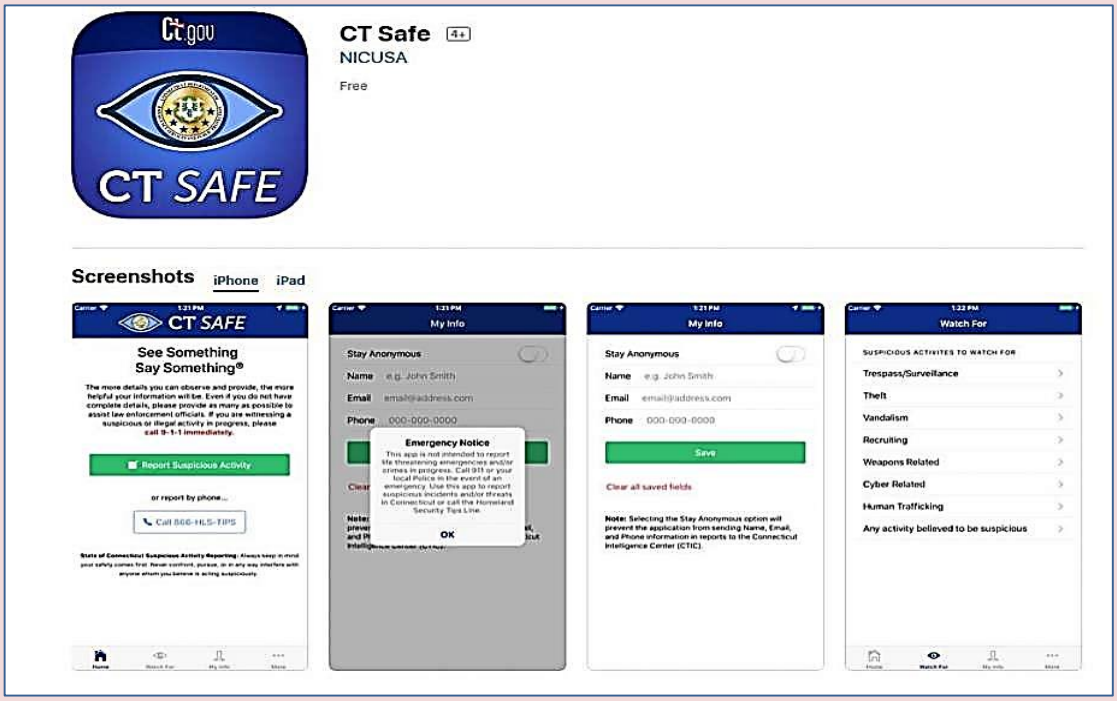
everyone – governments, companies and individuals alike – to set up rules and programs that support widespread cybersecurity, without waiting another 30 years.

Scott Shackelford *is Associate Professor of Business Law and Ethics; Director, Ostrom Workshop Program on Cybersecurity and Internet Governance; Cybersecurity Program Chair, IU-Bloomington, Indiana University.*

Connecticut Unveils New Mobile Phone App to Report Suspicious Activity to Authorities

Source: http://www.govtech.com/em/preparedness/Connecticut-Unveils-New-Mobile-Phone-App-to-Report-Suspicious-Activity-to-Authorities.html

Nov 07 – The state Department of Emergency Services and Public Protection has announced the release of a new mobile phone application where you can report suspicious activity to authorities.
The free app, it says, will engage "our public to assist in the security of the Homeland."



"The simple interface will allow the user to anonymously report unusual activity and even include photos in just a few clicks. The report is sent directly to Counter Terrorism watch personnel who are on-duty 24 hours a day. Join the team that keeps CT SAFE."
According to the description on the App Store, "The **CT Safe Mobile Application**, in collaboration with the Connecticut Department of Emergency Services and Public Protection, along with the Connecticut Intelligence Center, allows citizens of Connecticut to report on suspicious activities within their communities. Connecticut citizens can view and select suspicious activities from a list of predefined activities, elect the appropriate activity, and generate an email to the Connecticut Intelligence Center.
"The CT Safe Mobile Application integrates with Google Maps and a user's mobile device camera or photo library to send accurate location coordinates along with photos, assisting citizens reporting suspicious activities within their communities."
The Connecticut Intelligence Center is described as "the designated state fusion center, which is comprised of state, local and federal partners including the Division of Emergency Management and Homeland Security, Division of State Police, Department of Corrections, CT National Guard, Municipal police, FBI, U.S. Coast Guard, Office of the United States

Attorney, and the federal Department of Homeland Security. Personnel from additional state agencies are available as subject matter experts and liaisons to assist as needed."
Among the suspicious activities people should watch for are trespass/surveillance, theft, vandalism, recruiting, weapons-related, cyber-related, human tracking and "any activity believed to be suspicious."
"Always keep in mind your safety comes first. Never confront, pursue, or in any way interfere with anyone whom you believe is acting suspiciously."

To download:

- Android: https://play.google.com/store/apps/details…
- Apple: https://itunes.apple.com/us/app/ct-safe/id1437645620?mt=8

Why you may need to take this lie-detector test to catch TERRORISTS at the airport

Source: https://www.express.co.uk/travel/articles/1043018/flights-news-airport-security-terrorism

Nov 09 – AIRPORTS in Europe are set to introduce lie detector tests at the border to establish if passengers from outside the EU are terrorists or pose a terrorist threat to the country.
Those travelling through certain airports may be compelled to take a lie detector test with the aim of catching terrorists, criminals and illegal immigrants.
Passengers will be asked a number of questions while a special machine asseses the accuracy of their answers.

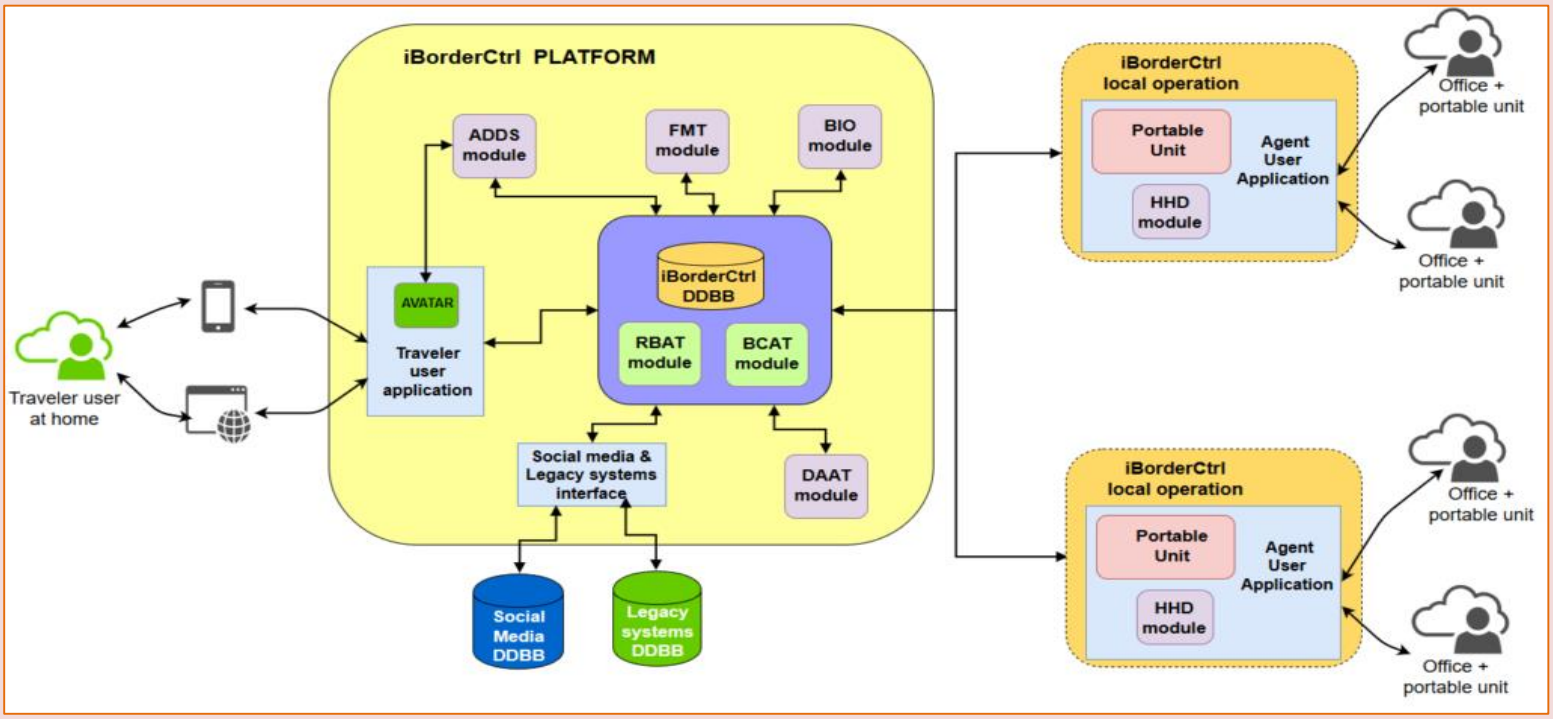
The questions will allude to the passenger's luggage and their identity. Would you be happy to undergo lie a detector test at airport security?

Airports in Europe are set to trial new Artificial Intelligence in a bid to fight terror and catch illegal immigrants entering the country.

Lie detector tests will be rolled out at airports in Hungary, Latvia and Greece as part of an EU-funded drive to fight crime.

The three nations all border non-European Union nations and will employ the new iBorderCtrl technology on travellers from outside the EU.
These fliers will have to use an online application to upload pictures of their passport, visa and proof of funds if they wish to travel.
They will then have to answer questions from a computer-animated border guard through a webcam.
They will be interrogated regarding their name, age and date of birth as well as the purpose of their trip or questions about their luggage.

According to New Scientist, some of these questions include: "What's in your suitcase?" and "If you open the suitcase and show me what is inside, will it confirm that your answers were true?"



The questions will be personalised to the traveller's gender, ethnicity and language.
The micro-expressions of those tested will be analysed to work out if they are lying.
Interviewees who are flagged as high-risk will undergo a more detailed check.
If iBorderCtrl identifies the person as telling the truth they will receive a QR code to let them pass the border.
If it suspects they are lying, biometric information will be taken, such as fingerprinting, palm vein reading, and face matching. This will recalculate the potential risk posed by the traveller.
A human border guard will then take over and will review the information and make an assessment.
"It is hoped that trials about to start in Hungary, Greece and Latvia will prove that the intelligent portable control system helps border guards reliably identify travellers engaging in criminal activity," said a European Commission statement.
"The trials will start with lab testing to familiarise border guards with the system, followed by scenarios and tests in realistic conditions along the borders."
The technology will not currently prevent anyone from crossing the border.

Why no cyber 9/11 for 15 years?

By Robert Graham (Errata Security)
Source: https://securityboulevard.com/2018/11/why-no-cyber-9-11-for-15-years/

Nov 02 – As a pen-tester who has broken into power grids and found 0dayss in control center systems, I thought I'd write up some comments. Instead of asking why one hasn't happened yet, maybe we should instead ask why national-security experts keep warning about them.
One possible answer is that national-security experts are ignorant. I get the sense that "national" security experts have very little expertise in "cyber" security. That's why I include a brief resume at the top of this article, I've actually broken into a power grid and found 0days in critical power grid products (specifically, the ABB implementation of ICCP on AIX — it's rather an obvious buffer-overflow, "cough" ASN.1 "cough", I don't know if they ever fixed it).
Another possibility is that they are fear mongering in order to support their agenda. That's the problem with "experts", they get their expertise by being employed to achieve

some goal. The ones who know most about an issue are simultaneously the ones most biased. They have every incentive to make people be afraid, and little incentive to tell the truth.

The most likely answer, though, is simply because they can. Anybody can warn of "digital 9/11" and be taken seriously, regardless of expertise. It's always the Morally Right thing to say. You never have to back it up with evidence. Conversely, those who say the opposite don't get the same level of press, and are frequently challenged to defend their abnormal stance.

Indeed, that's how this article by *The Atlantic* works. It's entire premise is that the national security experts are still "right" even though their predictions haven't happened, and it's reality that's somehow "wrong".

Now let's consider the original question.

One good answer in the article is that terrorists want attacks that "cause certain types of fear and terror, that garner certain media attention, that galvanize followers". Blowing something up causes more fear in the target population than deleting some data.

But something similar is true of the terrorists themselves, that they prefer violence. In other words, what motivates terrorists, the ends or the means? It is it the need to achieve a political goal? Or is it simply about looking for an excuse to commit violence?

I suspect that it's the later issue. It's not that terrorists are violent so much as violent people are attracted to terrorism. This can explain a lot, such as why they have such poor op-sec and encryption, as I've written about before. They enjoy learning how to shoot guns and trigger bombs, but they don't enjoy learning how to use a computer correctly.

I've explored the cyber Islamic dark web and come to a couple conclusions about it. The primary motivation of these hackers is gay porn. A frequent initiation rite to gain access to these forums is to post pictures of your, well, equipment. Such things are repressed in their native countries and societies, so hacking becomes a necessary skill in order to get it.

It's hard for us to understand their motivations. From our western perspective, we'd think gay young men would be on our side, motivated to fight against their own governments in defense of gay rights, in order to achieve marriage equality. None of them want that, as far as I can tell. Their goal is to get married and have children. Sure, they want gay sex and intimate relationships with men, but they also want a subservient wife who manages the household, and the deep family ties that come with spawning progeny. Thus, their motivation is still to defend the umma (the whole community of Muslims bound together by ties of religion) against the West, not pursue personal rights.

The point is, when asking why terrorists do and don't do types of attacks, their own personal motivations are probably pretty darn important.

Another explanation in that article is simply because Islamic hackers aren't good enough. This requires a more sophisticated discussion of what skills they need. As *The Atlantic* says in their article:

The most powerful likely barrier, though, is also the simplest. For all the Islamic State's much-vaunted technical sophistication, the skills needed to tweet and edit videos are a far cry from those needed to hack.

It's indeed not just "editing videos". Most hacker attacks you read about use un-sophisticated means like phishing. They are only believed to be sophisticated because people get confused by the results they achieve with the means with which they do it. For example, much of the DNC hack which had important consequences for our election was done simply by phishing the password from people like John Podesta.

A convincing cyber terrorism attack, such as causing a power black out, would take different skills — much rarer skills. I refer to my pentests above. The techniques used were all painfully simple, such as SQL injection from the Internet, but at the same time, it's a much rarer skill. No matter how simple we think SQL injection is, it takes a different skillset than phishing. It takes people more interested in things like math. By the time such skills are acquired, they get gainfully employed at a technical job and no longer have free time to pursue the Struggle. Phishing skills won't land you a high paying job, but web programming (which you need for SQL injection) will.

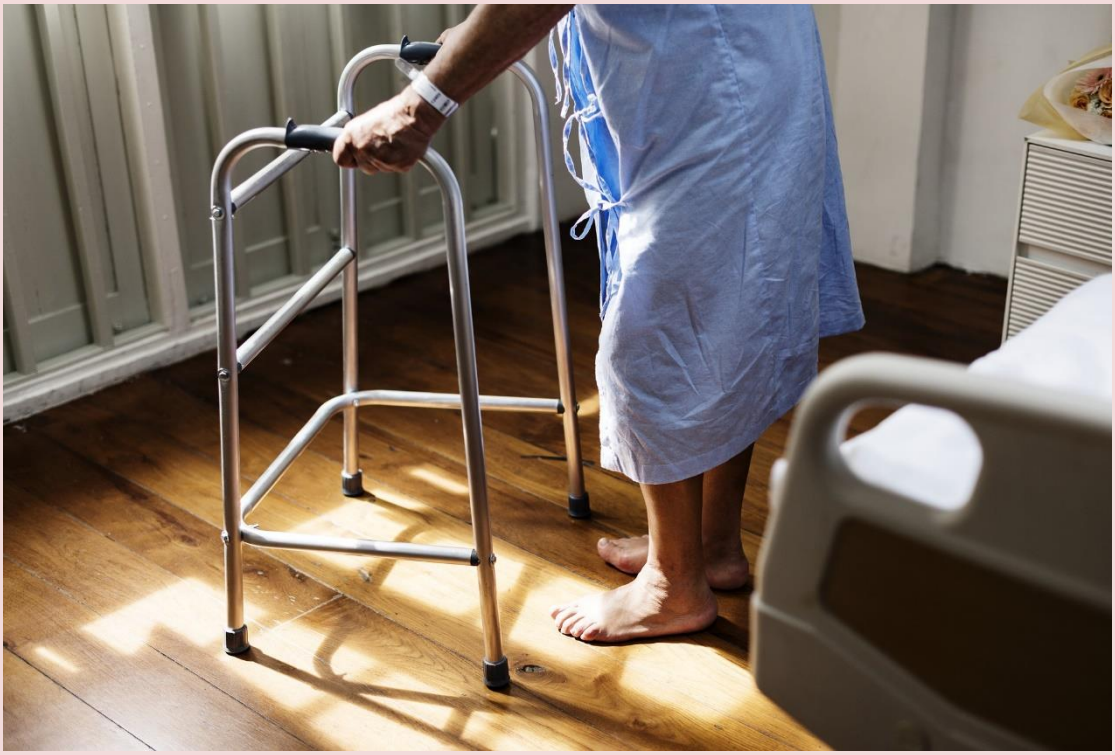
Lastly, I want to address the complexity of the problem. *The Atlantic* quotes Robert M. Lee of Dragos, a well-respected technical expert in this area, but I don't think they get the quote right. He points out the complexity of the power grid. What he means is not complex as in *hard* but complex as in *diverse*. There's 10,000 different companies involved in power production, long haul, distribution to homes, and so forth. Every state is different, every city is different,

and even within cities there may be multiple small companies involved.
What this means is that while hacking any one of these entities would be easy, it'd only cause a small-scale effect. To cause big-scale effects would require a much larger hacking campaign, of a lot of targets, over a long period of time. Chances are high that before you hacked enough for a convincing terror effect, they'd catch on to you, and take moves to stop you. Thus while any individual target is easy, the campaign as a whole is complex.
In the end, if your goal is to cause major power blackouts, your best bet is to bomb power lines and distribution centers, rather than hack them.

Conclusion
I'm not sure if I have any better answers, just more complex perspectives.
I think there are lots of warning from so-called "experts" who aren't qualified to make such warnings, that the press errs on the side of giving such warnings credibility instead of challenging them.
I think mostly the reason why cyberterrorism doesn't happen is that which motivates violent people is different than what which motivates technical people, pulling apart the groups who would want to commit cyberterrorism from those who can.
At least for power grid blackouts, while small attacks would be easy, the ones large enough to grab people's attention would be difficult, due to our power grid's diversity.

Healthcare Cyber Threat Is a Wake-Up Call for Patient Safety

By Omar Tisza
Source: https://www.hstoday.us/subject-matter-areas/cybersecurity/perspective-healthcare-cyber-threat-is-a-wake-up-call-for-patient-safety/



Nov 09 – Throughout our environment of interdependent critical infrastructure, the distributed and indiscriminate risk to patient safety in the health industry due to cybersecurity vulnerabilities is ever increasing. Consider going to your health service provider to receive lifesaving treatment and being turned away because the medical devices and electronic health records in the hospital have been incapacitated by ransomware, rendered unusable until the ransom is paid – and even if the ransom is paid, there is no guarantee the data held hostage will be operational or recoverable. This is the reality some health delivery organizations (HDO) experienced during the 2017 WannaCry cyberattack as it spread to more than 150 countries and affected more than 200,000

computers across the globe, as well as hospitals in at least two states. The most critical consequences of the lapse in quality of care were shouldered by the patients, whose lives were put at risk.

WannaCry Ransomware Attack: In May of 2017, ransomware – malicious software that threatens to make data unusable unless a ransom is paid, usually in bitcoin – was unleashed en masse on computers that were running outdated and unpatched versions of the Windows OS. A severely affected sector was healthcare, which includes HDOs, heath IT, medical device manufacturers, and other critical subsectors, as they rely on Windows to run myriad software to facilitate healthcare. As the cybersecurity posture of the heath sector had been long ignored, this cyberattack took advantage of the lack of protection. A notable example of the consequences took place within the jurisdiction of the UK National Health Service (NHS), which was forced to cancel appointments and deny treatment to patients because their systems were infected.

Recent global cyberattacks bring the cybersecurity concerns of the healthcare industry to the foreground, after being in the background of our healthcare security long enough for cyber threat actors to recognize and exploit our vulnerabilities. Cyberattacks such as brought widespread attention to myriad cybersecurity vulnerabilities in the healthcare sector. The impact and fallout of these attacks demonstrated the importance of improved preparedness and rapid response in the event of an incident. The light must shine on the smaller and lesser-resourced providers who need help enhancing their cyber posture. The security of the healthcare system is only as strong as its weakest link.

A significant portion of medium and small health providers don't consider information technology a strategic asset towards the system's success. In this light, and considering cybersecurity being a subcomponent of IT, cybersecurity is then an afterthought. The security program is an additional duty, and secondary priority, for IT staff already burdened with full-time jobs. To adequately prepare for and mitigate the cyber threats facing healthcare, health providers must select appropriate cybersecurity leadership and enable their efforts for an enterprise-wide strategy to protect patient lives and data. It is clear that health organizations must be creative and flexible in finding the appropriate leadership and staff, with appropriate skills, at the right price.

The common thread in cybersecurity between the health sector and other critical infrastructure is the potential for large-scale damage in the blink of an eye. Cyberattacks can unleash massive and widespread damage in multiple critical lifeline sectors; power grids can be shut off, water services can be denied, and health services can be interrupted with instantaneous maximum impact.

Petya/NotPetya Ransomware Attack: Akin to WannaCry, Petya ransomware encrypts the hard drive of computers until a bitcoin ransom is paid. It was first observed in 2016 and – soon after WannaCry – in June of 2017, an improved variant called NotPetya was the protagonist of another significant cyberattack aimed at major companies in multiple sectors, including healthcare, throughout Europe and the U.S.

To continue the enhancement of our security and resiliency, and improve patient healthcare, the health sector – industry and government together – must fully understand how healthcare technology and integration is continually evolving, and as such, providers have an ongoing obligation to manage medical technology, protect information systems and data, and safely provide patient care. But because of widespread healthcare infrastructure interconnectivity, such cybersecurity risk management cannot be done effectively in a vacuum. Our interconnected environment facilitates the spread of cybersecurity risks – across the supply chain and throughout the sector – and, as a result, our vulnerabilities are shared; my neighbor's risk is my risk. Cybersecurity necessitates the collaboration of all stakeholders. The patient care relationships that providers must serve are

based on patient safety, and patient safety increasingly requires cyber safety. Any regulatory mandate on healthcare must now be reviewed through this prism.

The Healthcare and Public Health Sector Coordinating Council's Cybersecurity Working Group has been actively involved in bringing the heath sector – our government and industry partnership – into a forum where subject matter experts and government leaders are encouraged to collaborate on myriad issues that threaten the security and resiliency of our cyber-posture. We have 13 task groups that deal with the pressures on the Healthcare and Public Heath Sectors (HPH), such as Supply Chain Risk Management, Medical Technology Cybersecurity, Intellectual Property Protection, and many more. We have two major cybersecurity guidance frameworks that are soon to be released: the Joint Security Plan (JSP) to increase the security and resilience of medical devices and health IT (mapped to the NIST Cybersecurity Framework), and the Top 10 Best Practices for minimum-level best practices in healthcare cybersecurity. Through these work products, and our active task groups, we strive to facilitate the collective mitigation of cybersecurity threats to the sector that affect patient safety, security, and privacy – and, consequently, national confidence in the healthcare system.

Patient safety has taken on a new dimension that demands our attention – the recognition that patient security requires cybersecurity. The health sector is striving to fortify the industry's immune system against a cyber epidemic that has become as infectious as a human epidemic. To implement a comprehensive security framework, the healthcare sector must work to get ahead of the threats facing the sector in a partnership with government and across critical healthcare subsectors like direct patient care, health IT, medical devices, pharmaceuticals, and health plans and insurance. This isn't just an IT security problem or a regulatory compliance problem, but one that needs the attention of health providers, chief medical officers, CIOs, general counsels, and the C-suite in general. In this way, we can collaboratively diagnose our cyber health, prescribe a regimen of treatment and move us closer to inoculation against an epidemic of cyber vulnerability.

Omar Tisza *graduated from American University in 2017 with a bachelor's in International Relations. He began his role as Jr. Risk Analyst at Gate 15 in 2018 and currently supports the Health Information Sharing and Analysis Center (H-ISAC) and the HSCC CWG under Executive Director Greg Garcia, former Assistant Secretary for Cyber Security and Communications at DHS.*

Using social media to weaken impact of terrorist attacks

Source: http://www.homelandsecuritynewswire.com/dr20181116-using-social-media-to-weaken-impact-of-terrorist-attacks

Nov 16 – Governments and police forces around the world need to beware of the harm caused by mass and social media following terror events. In a new report, leading counter-terrorism experts from around the world offer guidance to authorities to better manage the impacts of terror attacks by harnessing media communication.

"With social media, not only is the information immediate, but the public's access to information and conversations shape how an event is talked about," said Steven Chermak, MSU professor of criminal justice report contributor. "This can be dangerous when we can't discern fact from a panicked reaction."

The report, Minutes to Months, or M2M, assessed terror attacks in the United Kingdom, United States, Canada, New Zealand and Australia, with expertise from MSU, Western University in Canada, University of New South Wales, Sydney, and was spearheaded by Cardiff University's Crime and Security Research Institute, or CSRI.

MSU says that by reviewing all the published research on the role of media and social media in the wake of terror attacks, together with detailed case studies of specific incidents, M2M reveals insights on how media and social media coverage can increase the public harms of terrorism, and what works to mitigate such effects.

The M2M report provides recommendations to help authorities develop and execute strategies to manage the online fallout from a terrorist incident. The work was commissioned by the Five Country Ministerial Countering Extremism Working Group, which includes the governments of the UK, the U.S., Canada, Australia and New Zealand.

The research team found that terrorist attacks create shockwaves after the initial incident, as a wide range of voices compete through mainstream and social media. In fact, M2M found that communications after a terrorist incident often lead to a spike in hate crimes, extremism, and prompt damaging disinformation and rumors.

"People only know what they see or read, so the immediate panic social media – and then on the news – perpetuates rumors and creates fear. This is exactly what terrorists want," Chermak said. "The ongoing news in the days and weeks following attacks – and opinions and emotions through media – can continue the terror cycle."

Governments, police and others involved in public safety need to be ready to offer accurate, regular information to minimize negative fallout, the researchers said.

Terrorist violence, as the report explained, is intended to elicit intense and vivid reactions. Thus, by neglecting how to manage post-event situations is a current weak point in many governmental counter-terrorism frameworks.

The increasing volume of communication channels allows different groups to voice alternative interpretations of the same event, causing multiple narratives and accounts circulating in the post-event environment.

Martin Innes, director of the CSRI and lead author of M2M, recently issued a report that identified the systematic use of fake social media accounts spreading disinformation. The accounts, linked to Russia, amplified the public impacts of the four terrorist attacks that took place in the UK in 2017: Westminster Bridge, Manchester Arena, London Bridge and Finsbury Park.

"Over the past five years or so, both the mechanics and dynamics of terrorism and how it is reported via media sources, have altered dramatically," Innes said. "Over the same period, the logics of media and the information environment have been fundamentally transformed."

Because of these changes Innes believes that changing communication is the key to the post-attack wake of terror.

"Taking a pragmatic view, that despite the best efforts of police and security services, not all future plots will be prevented, developing an understanding of how any harms can be mitigated is an important undertaking."

The F-35's Greatest Vulnerability Isn't Enemy Weapons. It's Being Hacked

Source: https://www.popularmechanics.com/military/aviation/a25100725/f-35-vulnerability-hacked/

Nov 14 – The F-35 Lightning II can evade radar while infiltrating enemy airspace to deliver a knockout blow. It's a sophisticated, stealthy fighter with one big vulnerability—being hacked. As the plane finally reaches full production, the Air Force is racing to plug holes that could allow hackers to exploit the jet's connected systems—with disastrous results.

The aircraft itself is pretty secure. As *Air Force Times* explains, there are multiple layers of security surrounding the jet, including PIN numbers for individual pilots and secure authentication in crafting mission packages for uploading into the aircraft computer. A faraway hacker could not, for example, start up the aircraft and force its engine to explode, or cause the airplane to roll off the runway and crash.

F-35 pilots are fond of saying that the plane is as much computer as fighter jet.

But whether we're talking about a home computer, phone, tablet, or a hugely expensive fighter jet, vulnerabilities add up the more you're connected with the outside world. Much of

the F-35's strength lies in its ability to connect to the wider military and harness big data about the mission. The worldwide F-35 fleet is connected to at least two secure networks designed to maximize efficiency. The first is the Autonomic Logistics Information System, or ALIS, which keeps track of individual aircraft issues and the location of spare parts and equipment worldwide. Here's a Lockheed Martin video that describes ALIS:

Every F-35 squadron, no matter the country, has a 13-server ALIS package that is connected to the worldwide ALIS network. Individual jets send logistical data back to their nation's Central Point of Entry, which then passes it on to Lockheed's central server hub in Fort Worth, Texas. In fact, ALIS sends back so much data that some countries are worried it could give away too much information about their F-35 operations.

Another networking system is the Joint Reprogramming Enterprise, or JRE. The JRE maintains a shared library of potential adversary sensors and weapon systems that is distributed to the worldwide F-35 fleet. For example, the JRE will seek out and share information on enemy radar and electronic warfare signals so that individual air forces will not have to track down the information themselves. This allows countries with the F-35 to tailor the mission around anticipated threats—and fly one step ahead of them.

Although the networks have serious cybersecurity protections, they will undoubtedly be targets for hackers in times of peace, and war. Hackers might try to bring down the networks entirely, snarling the worldwide logistics system and even endangering the ability of individual aircraft to get much-needed spare parts. Alternately, it might be possible to compromise the integrity of the ALIS data—by, say, reporting a worldwide shortage of F-35 engines. Hackers could conceivably introduce bad data in the JRE that could compromise the safety of a mission, shortening the range of a weapon system so that a pilot thinks she is safely outside the engagement zone when she is most certainly not.

Even the F-35 simulators that train pilots could conceivably leak data to an adversary. Flight simulators are programmed to mirror flying a real aircraft as much as possible, so data retrieved from a simulator will closely follow the data from a real F-35.

In an interview with *Defense News*, Brig. Gen. Stephen Jost, director of the Air Force F-35 Integration Office, says there are "a lot of nodes of vulnerability that we're trying to shore up." Not only is the worldwide networking system vulnerable, wireless systems used to support the F-35 could also be points of entry for hackers.

F-35 pilots are fond of saying that the plane is as much computer as fighter jet. While the use of computers and worldwide networking is a benefit to all of the jet's operators, the U.S. military and F-35 customers worldwide must be sure the aircraft—and the equipment that supports it—is properly armored against cyber threats. The alternative could be the jet's greatest advantages being quietly turned against it, the extent of the damage known only once the shooting starts.

Pentagon Researchers Test 'Worst-Case Scenario' Attack on U.S. Power Grid

Source: https://www.nextgov.com/cybersecurity/2018/11/pentagon-researchers-test-worst-case-scenario-attack-us-power-grid/152803/

Nov 13 – The team of grid operators had spent days restoring power when a digital strike took out one of two operational utility stations. The other utility was also under attack.

A month had passed since all power in the region was taken down by a devastating cyberattack. It had been a grueling six days restoring power across two electrical utilities and to the building deemed a critical national asset by the Secretary of Energy.

The cyber strike hadn't forced the team back to zero, but it wasn't far from it.

Just moments ago, the two electric utilities had been working in concert, delivering reliable and redundant power to the critical asset. Now one utility was down for the count and the other was under attack.

The grid operators' only chance to restore power to the asset would be to route it, substation by substation, from the utility that was still operating. The team of cybersecurity researchers assisting the grid operators would have to use every piece of technology and know-how they had to ensure that utility stayed powered up, trustworthy and malware-free.

The Defense Advanced Research Projects Agency exercise, which took place from Nov. 1 to Nov. 7, was fictional, but it was designed to mimic all the hurdles and uncertainty of a real-world cyberattack that took out power across the nation for weeks on end–a scenario known as a "black start."

To add realism, the exercise took place on Plum Island, a federal research facility off the north fork of Long Island, where DARPA researchers were able to segregate a portion of the island on its own electric grid.

Over the course of the seven-day exercise, more than 100 people gathered on the island, filling every necessary role to mimic an actual black start.

At the center of the exercise was a team of grid operators from electric utilities across the nation, which was in charge of restoring and sustaining power.

At its most basic level, their job involved creating initial power transmissions at both utilities using a diesel generator, then building cyber-secure "crank paths" through a series of electric substations that would increase the transmissions' voltage until they were capable of powering the two utilities and delivering redundant power to the exercise's critical asset.

Get the latest federal technology news delivered to your inbox.

email

Meanwhile, another team of DARPA-funded cyber researchers from seven different industry groups used custom built technology to keep the grid operators' efforts protected from cyber adversaries.

A third DARPA-funded team took the role of the cyber adversaries, throwing a wrench into the good guys' efforts every time they seemed to be getting ahead.

"We have a bunch of things that try to make this as painful as possible for everyone," project leader Walter Weiss told reporters on a rainy Tuesday, the sixth day of the exercise. "How do you actually keep the smartest people in the world busy for a week? That takes effort."

Try, Try Again

The Plum Island exercise is the fourth black start exercise led by **DARPA's Rapid Attack Detection, Isolation and Characterization Systems, or RADICS**, program, which Weiss leads. The first two exercises were conducted in research labs. The third one took place on Plum Island but on a smaller scale and without public observers.

DARPA plans to continue the exercises every six months until the RADICS program expires in 2020, Weiss said. After that, hopefully, the project will continue under the Energy Department or another federal agency, he said.

The RADICS exercise doubled as the second phase of an Energy Department exercise called Liberty Eclipse. The first phase of that exercise, which took place in October, was a tabletop exercise during which government and industry officials game planned policy options after a massive cyberattack against the grid.

That exercise ended with the fictional president declaring a grid emergency and the energy secretary using a power first formalized earlier this year to issue emergency orders to get the grid back up and running.

One of those orders—to get redundant power to the critical asset on Plum Island—marked the beginning of the on-island exercise this month.

While Weiss and project organizers pushed for realism in the exercise, they kept some details vague. The utilities were dubbed simply Utility A and Utility B. The scenario doesn't name the U.S. adversary that launched the grid-crippling cyberattack. Nor does it identify the "critical asset" that grid operators must keep running.

In a real-world attack, that critical asset might be a hospital, a military base or any other building that's critical for the nation's functioning during an emergency.

In the exercise, the asset was an aged brick building outfitted, on an upper level, with five multi-colored air dancers—the colorful, fan-powered, headbanging nylon tubes that often adorn car dealerships and cellphone stores.

Weiss described the air dancers as "high visibility power indicators." When the asset was receiving power, the dancers would do their thing and the grid operators, observing from a distance, could breathe easy. If the dancers started slouching, they knew something was wrong.

A Very Particular Set of Tools

The cyber researchers, who hailed from the National Rural Electric Cooperative Association, BAE Systems, Perspecta Labs and elsewhere, brought three main types of technology to the DARPA exercise:

- Tools that provide situational awareness about what portions of the grid cyberattackers had infected with malware and which parts remained secure.
- Tools that isolated healthy parts of the grid so they couldn't be infected.
- Tools that assessed and diagnosed the nature of the cyberattack that brought the grid down.

The researchers' primary focus was testing, communicating about and bypassing infected parts of the power grid without creating any digital connections that could carry malware infections into the tools themselves or into post-attack portions of the grid.

Their situational awareness tools, for example, ignored digital signals from the grid and relied on basics physics tests that are impossible to hack. Their cellphones and other communications systems operated on local networks that were segregated from the internet and broader telecom networks.

The goal wasn't for the tools to compete against each other, Weiss said, but to test how effectively researchers and grid operators could use the tools after a truly devastating cyberattack.

In some cases, the tools didn't perform as planned. In other cases, they worked well, but didn't provide information in a format that was most useful to grid operators, Weiss said. That's feedback the teams can use to rejigger their tools for the next exercise in six months, he said.

In other cases, the tools worked but were stymied by other factors that might also affect a real-world grid attack.

Researchers readied a weather balloon, for example, that could fly 500 feet above the island and detect acoustic hum and other indicators of where electricity was and wasn't flowing properly. When reporters visited on the sixth day of the exercise, however, the balloon was grounded by persistent rain.

Earlier in the exercise, researchers spent an entire day chasing what they believed was a red team cyberattack but was actually just an anomaly in grid operations, Weiss said.

"It was just a giant false positive for a day," he said. "If you take a bunch of researchers and stick them on an island like this, they're going to get pretty paranoid."

Finally, many times the tools worked effectively but needed the researchers, who were based in nearby Orient Point, Long Island, to go out and tinker with them or to help the grid operators troubleshoot, Weiss said.

In the exercise, that meant a delay of an hour or two while researchers waited for the next ferry to the island and made their way to the utility or substation. In a real-world black start, however, that could mean a wait of days or more while a too-small cadre of harried cyber experts zipped from place to place.
Weiss's challenge for the cyber researchers, he said, is that their tools should be so user-friendly by the final exercise in 2020 that grid operators—or anyone else without specialized cyber training—will be able to use them to re-establish power by simply reading a manual.
In a real-world grid attack, for example, National Guard units might be deployed to re-establish power to specific assets or to restart power in specific sectors, Weiss said.

And There Was Light
By the end of the seventh day, despite ongoing ransomware and other cyberattacks and the loss of power at Utility B, grid operators were able to re-establish power at the critical asset, Weiss told *Nextgov* in an email after the exercise.
DARPA's main research focus for the exercise wasn't the grid operators' success or failure, however, but how well the tools withstood various impediments and assaults by the red team of cyberattackers, Weiss said.
If the grid operators and cyber researchers were over-performing, the red team would automatically throw something more difficult at them, Weiss said. That meant the grid operators were nearly foreordained to meet their goal by a whisker's margin.
The red team socked away about 10 days of mischief for the seven-day exercise, Weiss said, so it could match the grid operators' and researchers' best work and still have something left over for the next exercise in six months.
"Our goal is to be dynamic," he said. "We don't want them to be perfect. We want to find the limits of the tools. We're driving them to a point where we see how far they can get and then we beat them back down."
That may sound sadistic, but it mirrors what grid operators and their cyber helpers are likely to face in a real-world massive attack by a U.S. adversary.
"If you look at advanced persistent threats, they get more tools, they don't get less," Weiss said, using a common phrase for highly skilled nation-state-backed hacking teams from Russia, China, Iran and elsewhere.
If the tools can withstand that sort of battering, Weiss said that means they can be useful in less extreme situations.
"We exercise with that absolute worst-case scenario where everything's gone wrong, everything's failed for a month and ask how are our tools still relevant," Weiss said. "If we can prove a tool works when everything else is broken, that gives us more confidence."

What is Hidden behind Streetlights?

Source: https://i-hls.com/archives/86955
Nov 23, 2018

Nov 23 – The use of surveillance cameras in urban environments has been widening. Smart city applications for traffic management, pedestrian counting etc. have become more prevalent in various countries around the globe. China has been reputed as a leading player in this field. Now, US authorities have been apparently hiding surveillance cameras in streetlights? The US Drug Enforcement Administration (DEA) and Immigration and Customs Enforcement (ICE) have hidden an undisclosed number of covert surveillance cameras inside streetlights around the country, federal contracting documents reveal.
Government procurement data reveal that these authorities have paid companies for "video recording and reproducing equipment." It's unclear where the DEA and ICE streetlight cameras have been installed, or where the next deployments will take place.
Christie Crawford, who owns one of the companies that supply these services, Cowboy Streetlight Concealments, told qz.com: "We do streetlight concealments and camera enclosures. Basically, there's businesses out there that will build concealments for the government and that's what we do. They specify what's best for them, and we make it."

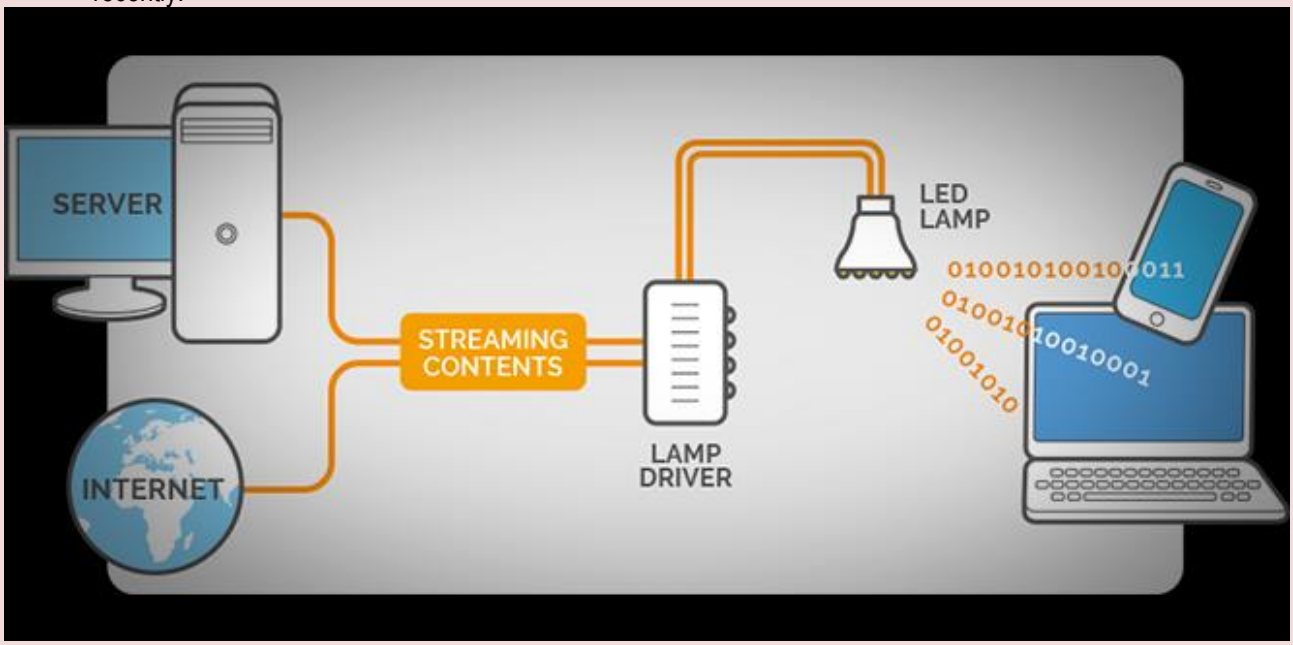
In addition to streetlights, the DEA has also placed covert surveillance cameras inside traffic barrels, a purpose-built product offered by a number of manufacturers. The DEA operates a network of digital speed-display road signs that contain automated license plate reader technology within them.

Chad Marlow, a senior advocacy and policy counsel for the American Civil Liberties Union, says efforts to put cameras in street lights have been proposed before by local law enforcement, typically as part of a "smart" LED street light system. "It basically has the ability to turn every streetlight into a surveillance device, which is very Orwellian, to say the least," Marlow told Quartz.

Secure Internet Connectivity Now Available via Luminaire

Source: https://i-hls.com/archives/86978

Nov 24 – Light will receive a strategic meaning as the new intelligent language in the digital age, especially with the arrival of the Internet of Things (IoT). A new technology using high-quality light-emitting diode (LED) lighting to obtain a broadband Internet connection through light waves has been introduced recently.



While radio frequencies are becoming congested, the visible light spectrum is an untapped resource with a large bandwidth suitable for the stable simultaneous connection of a vast array of Internet of Things devices.

Signify, a lighting company for IoT, has revealed its Light Fidelity (LiFi). The company said the technology is undergoing testing in 20 countries around the world to determine its performance and capability. The entry of LiFi can be a response to cybersecurity growing concerns in different sectors, such as business, defense and security.

Signify is the first global lighting company to offer LiFi-enabled luminaires from its existing office lighting portfolio.

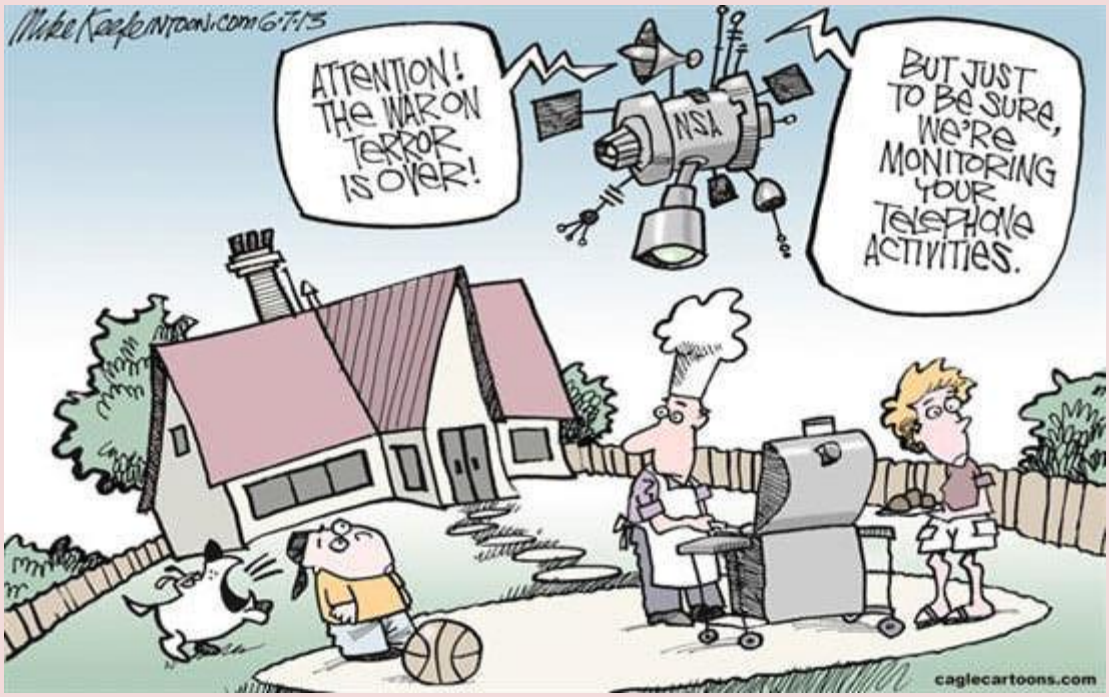
Under a LiFi network, access is only given to users within a room of a building. "It is a reliable network that gives stability to the data for the users despite the number of users. It is an alternative solution that gives stable connection despite the presence of radio frequency-sensitive areas with poor or no wireless fidelity [Wi-Fi] connection," explained Ed Huibers, head of business development of LiFi.

Although it is similar to Wi-Fi, LiFi technology is a two-way, high-speed wireless technology that uses light waves instead of radio waves to transmit data. Signify's office luminaires enabled with LiFi technology from Signify provide broadband connection with a speed of 30 Megabits per second without compromising lighting quality. With 30 Mbps a user can stream simultaneously several HD quality videos while having video calls, according to businessmirror.com.

Where can LiFi be utilized? The technology offers its advantages in places where radio frequencies may interfere with equipment, such as in hospitals, or where Wi-Fi signals cannot reach or are weak, such as underground. Other user cases include environments demanding high security; for example, the back office of a financial institution or government service. Moreover, the technology offers an enhanced security as light cannot pass through solid walls and a line-of-sight to the light is needed to access the network.

Each luminaire is equipped with a built-in modem that adjusts the light at speeds imperceptible to the human eye. The light is detected by a LiFi USB key/dongle plugged into the socket of a laptop or tablet (in the future such technology will be built into laptops and devices). The LiFi USB dongle returns data to the luminaire through an infrared link.

As LiFi has 10,000 times the spectrum of Wi-Fi, this technology enables quality, energy-efficient LED light and a highly secure, stable and robust connection.




ICI
International
CBRNE
INSTITUTE
CBRNE-Terrorism Newsletter
W
O
M
D
C2BRNE
DIARY
EMERGENCY
RESPONSE

Gameday Security NCS

Fall 2018

Source: https://issuu.com/ncs4southernmiss/docs/gameday_security_fall_2018?

Two interesting articles:

DETECTION PROTECTION

After successful implementation in the NFL and MLB, metal detectors are starting to find a much-needed home on the lower levels.

Earlier this year, a group led by Louisiana State University President F. King Alexander passed a mandate that **all SEC** (Southeastern Conference Commissioner) **football stadiums have metal detectors in place by 2020.**

STOP THE BLEED

These three simple steps to controlling bleeding could mean the difference between life and death.

BY LINDSAY GIETZEN & DARCY LEUTZINGER

Bleeding control curriculum is organized into three simple steps, and it should be implemented in every public establishment.

1. The first step in bleeding control is **ALERT**.
2. The second step in bleeding control is **BLEEDING**. The provider will need to identify the type and source of bleeding.
3. The third and final step in bleeding control is **COMPRESSION**.

It is everyone's responsibility to become a first responder and make a difference.

New Virtual Training Gives First Responders and Educators an 'EDGE' on School

Source: https://www.dhs.gov/science-and-technology/news/2018/11/01/news-release-new-virtual-training-gives-fr-and-educators-edge

Nov 01 – First responders and educators now have a new, free tool at their disposal to help ensure the safety of our nation's schools, as well as the students and faculty within them.

Developed by the Department of Homeland Security (DHS) Science and Technology Directorate (S&T), the U.S. Army Simulation and Training Technology Center (STTC), and Cole Engineering Services Inc. (CESI), the Enhanced Dynamic Geo-Social Environment (EDGE), a virtual training platform, allows teachers, school staff, law enforcement officers, and others tasked with school security to create and practice response plans for a wide range of critical incidents.

"When it comes to the safety and security of students, there is no holding back," said William N. Bryan, S&T Senior Official Performing the Duties of the Under Secretary for Science and Technology. "In many cases, school staff are the 'first responders' at the scene of an on-campus incident. We developed EDGE to help them prepare, so they have a new resource literally at their fingertips. By using EDGE to train, they can know how to act swiftly, decisively, and in collaboration with local emergency responders if and when something does happen."

Built on the Unreal 4 gaming engine, which powers popular video games like Fortnite and Street Fighter 5, EDGE allows first responders and educators to role-play complex scenarios in a virtual environment, improving and reinforcing coordination, communication, and critical decision-making skills. Users control avatars representing their real-life role—teachers, administrators, school resource officers, local law enforcement, and more—to execute a number of training scenarios of their own creation. The EDGE environment can be used to train for any type of incident, from parental custody disputes to potential bomb threats, an active shooter or other critical incident on campus.

"While EDGE leverages the best that gaming technology has to offer, it is important to note that it is *not* a traditional video game," said S&T EDGE Program Manager Milt Nenneman. "There are no winners or losers, and there are no pre-programmed situations to react to—EDGE allows agencies to create their own lesson plans, each with different outcomes based on the actions users take in the environment. There is some artificial intelligence programmed in, but for the most part users control the reactions of their own avatars under the guidance of a training manager."

"The level of threat and response can vary depending on specific training goals," agreed Tami Griffith, engineer at the STTC in Orlando. "This is an area that can turn chaotic quickly. The EDGE simulation allows educators and first responders to train in a school environment with a wide range of threat types, which is true to everyday life. The real value here is in the cross-response coordination. The more you train and prepare, the better the outcome."

EDGE was intentionally developed as a tool to supplement existing trainings, like field drills or tabletop exercises; because it is user-driven, it reflects the policies and procedures already in place in communities and school districts. The EDGE team worked with stakeholders across the country to incorporate practitioner feedback into the training platform, most recently this summer and fall in school districts in Arizona, Ohio, and Florida, as well as in West Orange, New Jersey, where the actual school modeled in EDGE can be found.

"One of the things I say over and over is there isn't enough training for educators in many aspects of school safety," said Dr. Amy Klinger, Director of Programs for the Educator's

School Safety Network. "This tool strikes a balance between 'we have to train for the worst-case scenario' and the more likely scenarios that we're going to encounter every day. We know that violence occurs in schools, we know that you are going to have aggressive behavior and situations that don't necessarily involve gun violence but that involve some other response that needs to occur," Klinger added. "EDGE gives educators an opportunity to immerse themselves in it, make decisions, analyze those decisions and think 'OK, what would I have done differently?' And then you can do it differently. As opposed to a one-time training, where you think 'I wish I had done this.'"

This is the second EDGE environment to be made available. The initial version, released in June 2017, featured a multi-story hotel environment enabling first responders of all disciplines to train together for a coordinated response to active shooter and other critical incidents. The new school environment is available at no cost to fully vetted response agencies and education institutions via the CESI EDGE Help Desk at (877) EDGE-011 or www.cesiedgetraining.com.

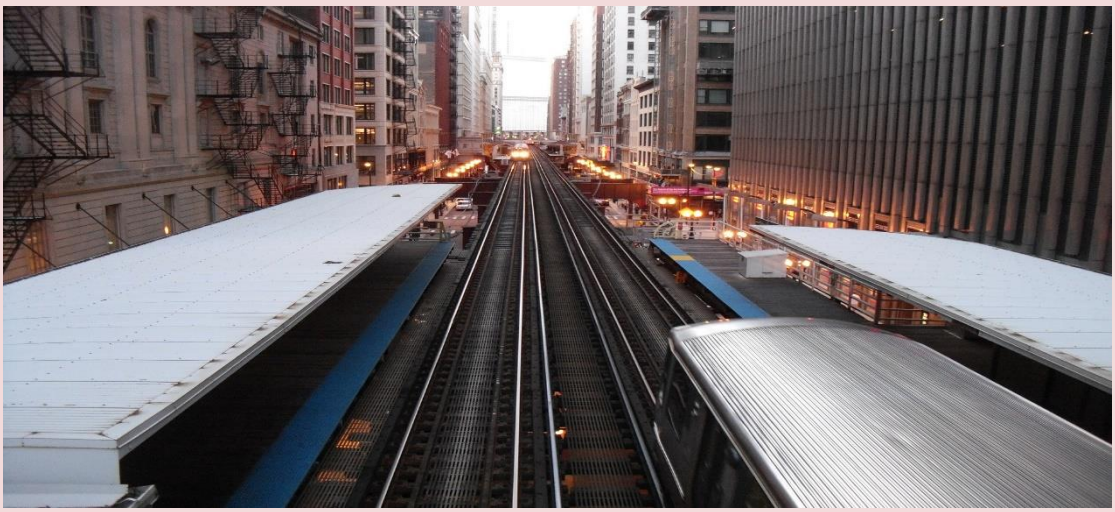
"You can never prepare enough. Using tools like EDGE—it can't hurt, it can only help," said Lieutenant John Morella of the West Orange, New Jersey Police Department. The school depicted in the EDGE environment was modeled after a middle school in West Orange, and Morella himself provided critical input for EDGE's research and development since its infancy. "[EDGE is] another tool in our toolbox, and it will allow us to do more training and be more interactive—not only on the police side, but the education side as well. It allows us to reset, go through multiple scenarios in a much shorter period of time, and it's more efficient and cost-effective. For this to be free, and for [responders and educators] to use this as often as they want…that's a home run."

For general EDGE information, visit https://www.dhs.gov/science-and-technology/EDGE or contact first.responder@hq.dhs.gov.

Cross-Sector Collaboration Critical in Protecting Urban Environment

By Thomas Henkey

Source: https://www.hstoday.us/subject-matter-areas/infrastructure-security/perspective-cross-sector-collaboration-critical-in-protecting-urban-environment/



Nov 02 – As any security director or emergency manager can testify, complex incidents and emergencies require a wide range of resources and skill sets. 2017 proved to be one of the most challenging years in recent memory for safety professionals across North America, with hurricanes, wildfires, flooding, acts of terrorism, mass shootings, and more.

What each and every one of these large-scale incidents had in common was that all demanded a unified response to protect people and infrastructure. These examples required cross-sector collaboration for effective response and recovery – public sector, private sector, and nonprofit sector.

At its core, collaboration is "to work jointly on an activity, especially to produce or create something." Ultimately, collaboration may be seen as a force multiplier – magnifying the impact of multiple organizations, units, or assets by combining available resources and skill sets. In an urban area, the immediate impacts and cascading effects of a disaster are magnified by a concentration of people and infrastructure.

Best Practices

A number of lessons learned during the initial start-up phase of a new collaborative effort are particularly relevant. A new organization including elements of critical infrastructure from across multiple sectors can greatly improve its chances at long-term survival and ongoing positive impact by considering a few key foundational actions.

- Set common objectives: Begin by assessing risk to help establish a group of core, overarching strategic objectives.
- Establish structure and operating parameters: A basic organizational format for the collaboration must be established, such as a committee, task force, or working group.
- Identify potential partners: Select potential contributors to reach the strategic objectives, drawing upon all sectors and multiple organizations.
- Set meeting/planning frequency and format: Participants must collectively decide how often to meet and in what format (i.e. teleconference, Skype, in-person, or some combination).
- Identify specific goals and projects: Attainable and tactical project goals with realistic timelines should be established to advance the strategic objectives.

Starting a cross-sector collaborative effort is a challenging endeavor. Yet multiple successes over a period of time will be required to keep it going. Highly successful collaborative bodies often share a number of readily identifiable traits or characteristics.

- Meeting on a regular basis: Staying on schedule by communicating on a regular basis is vital to advance both short-term and long-term project goals (and is made considerably easier by technology).
- Tangible progress and outcomes: Specific goals and specific results display value to both internal and external members and encourage future participation.
- All members contribute: Successful collaborative organizations do not include "free rides" – all active stakeholders must bring resources or skills to the group.
- All members benefit: Stakeholders must also be rewarded for participation via tangible project outcomes and takeaways.
- New tasks and projects: When one project nears completion, the group should identify another to take its place – no meeting for the sake of meeting.

To further complicate such collaborative efforts, recall that we are attempting to implement and sustain such efforts across the full cycle of emergency management. Truly effective cross-sector cooperatives will be active in prevention, preparedness, mitigation, response, and recovery. This model embraces an "all-hazards" approach, addressing natural, human-caused, and hybrid threats – including acts of terrorism or criminal sabotage.

Several less-tangible elements can contribute to a collaborative infrastructure-protection effort truly gaining traction within its membership and jurisdiction(s).

- Personalities matter nearly as much as qualifications: Skill sets are vital, but temperament may be just as important.
- Training and exercises will increase interaction: We tend to play how we practice, so involvement in a rigorous training program is highly beneficial.
- An association of associations, network of networks: The ideal collaborative member will in turn represent his or her entire network of similar organizations (law enforcement agencies, hotel operators, etc.).
- Interface with the local emergency operations center: The organization should have direct contact with their EOC, and ideally a seat at the table to rapidly provide and/or disseminate information.

Case Study

Chicago provides an example of collaboration in a major American jurisdiction. As in many large cities, cross-sector collaborative efforts are vital to Chicago's homeland security and emergency management posture. With a population of just under 3 million, Chicago is the third-largest city in the nation, and the largest in the Midwest/Great Lakes regions and FEMA Region V.

Local oversight and guidance is provided by the Office of Emergency Management and Communications (OEMC). In 2010, the OEMC launched a collaborative effort called the Critical Infrastructure Resiliency Task Force (CIRTF). The original group consisted of public-sector agencies, private-sector critical infrastructure owners and operators, and active nonprofits.

In 2012, Chicago hosted the North Atlantic Treaty Organization (NATO) summit, demanding immense and detailed planning for hazards including civil unrest and terrorism. As a part of the after-action process, the CIRTF expanded and evolved as the Chicago Public-Private Task Force (CPPTF). The organization meets monthly, and operates under two co-chairs, one nominated from the public sector and one from the private sector.

Current CPPTF membership Includes:

- Fire/EMS
- Police
- Public health
- Emergency management (current co-chair)
- Hospitals
- Cultural properties
- Colleges/universities
- Commercial buildings
- Retail buildings
- Financial firms (current co-chair)
- Apartment buildings
- Hotels/tourism

Tangible projects remain crucial. Specific ongoing collaborative efforts include the Business Recovery Access Program (BRAP) credentialing project, Chicago Central Business District evacuation/shelter plans, joint cross-sector drills and exercises, and joint coordination of large-scale special events.

This preparedness process must include both pre-planned and spontaneous events.

OEMC leads multi-departmental and cross-sector planning and intelligence-sharing efforts for large-scale special events such as the Lollapalooza music festival and the Chicago Marathon. The city's emergency operations center (EOC) coordinates events in real time, and includes a seat designated for a qualified private-sector representative.

Still very much an active group, and a work-in-progress, the CPPTF has already proven highly valuable to members, and to their professional networks throughout Chicago.

Conclusions

Cross-sector collaboration is not a convenience for urban centers – it is a necessity. Collaboration begins with common objectives and an established structure. Traits of successful public-safety efforts include regular communication, tangible progress and outcomes, with input and benefit for all stakeholders.

Thomas Henkey *served for six years as Senior Emergency Management Coordinator for the City of Chicago, where he was responsible for disaster planning and response, as well as special events, physical-security, infrastructure, transportation, and homeland security and antiterrorism analysis. Mr. Henkey also has nearly 15 years of experience in a range of private-sector and nonprofit safety and security management roles. In 2017, publisher Elsevier released his new text Urban Emergency Management. He is currently the Director of Emergency Management for Titan Security Group, and an adjunct instructor at DePaul University's School of Public Service. Mr. Henkey is a Certified Emergency Manager (CEM), a Certified Institutional Protection Manager, and a member of the International Association of Emergency Managers, the ASIS Cultural Properties Council, the Chicago Public-Private Task Force, and the Chicago*

Council on Global Affairs. He is the vice-chair of the Chicago Cultural Properties Security Group, as well as vice-chair of the BOMA-Chicago Preparedness Committee. Mr. Henkey holds undergraduate degrees from St. Louis University, and a Master's Degree in Emergency and Disaster Management from American Military University.

He got mugged, then revamped 911 for the next generation

By Brian Blum

Source: http://www.homelandsecuritynewswire.com/dr20181113-he-got-mugged-then-revamped-911-for-the-next-generation

Nov 13 – Amir Elichai was walking along the beach in Tel Aviv when he was approached by strangers who demanded his wallet. He complied, and as soon as he was safe, he called Israel's emergency services system.

"The response time was terrible," he recalls, leaving the muggers plenty of time to flee. "The technology was not at all up to date." So Elichai decided to change the situation.

Four years and $24 million later, Elichai's company, Carbyne, has re-engineered the infrastructure for 911 services from the ground up, to take advantage of all the innovations that have come along in the 20 to 30 years since most emergency systems were built.

Those innovations include the ability to see the location of a caller on a map, to chat by text if a voice call is not possible, to use VoIP (Voice over IP) services like WhatsApp and Skype, and to stream video so the 911 operator can see what's happening in real time.

Carbyne (formerly known as Reporty) now has customers in 30 cities in the United States, Mexico, Europe, Israel and Singapore. The latest customer, in the city of Huixquilucan de Dogollado, Mexico, came online in September.

"Listening to the call-takers and the PSAP [public safety answering point] staff as they watched the pins drop [on the Carbyne 911 map] within a few meters of where the callers were, and the video upload on their screens was amazing," says Raymundo Sánchez López, Carbyne's regional director of sales for Mexico.

Carbyne has a staff of 65 in three offices – Tel Aviv, New York and Mexico. The company's chairman is former Israeli Prime Minister Ehud Barak.

Could be built into Waze

Emergency call systems aren't particularly sexy – they're the kind of services you don't think about until you need them. That was one reason why Founders Fund, which joined the company's August Series B funding round of $15 million, became interested.

"I'm looking for businesses that aren't massively competitive and Carbyne stands alone in a really unpopular industry," Trae Stephens, a partner at the firm who is leading the investment, told the website TechCrunch.

Popular or not, it's a big market: In the US alone, 240 million urgent help calls are made each year.

Legacy 911 systems were built to work with fixed-line phones. But these days, up to 80 percent of all emergency calls come from mobile phones, which can provide a far richer range of data.

Carbyne's C-Now app for Android or iOS phones is live in 161 countries and works with Carbyne's backend call-handling system, which tracks and stores events (the latter for up to seven years as required by law in many locations).

If you don't have the app installed, Carbyne's C-all technology will take over your device, allowing the emergency-services team to access your phone's camera and microphone.

Elichai demonstrated the system for ISRAEL21c. He sent us a text link, we clicked on it, and Elichai could then see and hear everything happening on our end. It was a bit creepy but effective.

Clicking the link gives Carbyne the consent it needs in some countries. That's particularly important in Europe, where new privacy regulations limit what a tech company can do with your data.

The company is planning to launch a gateway product that will allow third parties — like Uber or Waze — to integrate the technology instead of requiring users to download and launch Carbyne's C-Now app.

While Elichai says that Carbyne's ultimate goal is to "replace all the legacy providers," its C-Lite service plugs directly into legacy 911 services and allows advanced features such as location and video to appear in a floating window on top of the operator's existing interface.

Remote installation

Despite investor Stephens' description of the 911 business as "an unpopular industry," Carbyne is not without competitors. The biggest is RapidSOS, which bills itself as a "bridge" between mobile phone calls and legacy 911 PSAP services. During the recent tropical storm disasters in Puerto Rico, Texas and Florida, RapidSOS was able to take over when the legacy systems failed.

Elichai says that Carbyne has an advantage over RapidSOS in that it can be a full replacement for a legacy 911 system and is super easy to install. In many cases, swapping out an existing system with Carbyne can be done remotely because Carbyne's smarts are in the cloud, not in onsite computers.

"We can have your new system up and running in one day," Elichai tells ISRAEL21c. While Carbyne will usually send someone to a customer's 911 center, "it's for training, not for connecting wires or configuring computers."

Carbyne can be used for more than classic 911 emergency services.

A municipality can allow citizens to report road problems and traffic jams. An educational institution can connect students to a call center, whether that's an emergency button on the playground or while out on a field trip. Colleges, corporate campuses and public parks can also take advantage of Carbyne's next-generation communications.

And when third parties plug in, the sky's the limit. It could be "a signal generated by a web-based monitor in a child's room," Elichai suggests, or even a heart monitor broadcasting the alert.

For first-responders, though, the benefit is clear: Carbyne says its customers see response and dispatch times improved by some 65% on average.

That might not have helped Elichai get his money back on the Tel Aviv beach but it could have stopped the muggers from striking again.

***Brian Blum** writes about startups, pharmaceutical advances, and scientific discoveries for Israel21c.*

Community Emergency Response Team

Source: https://www.ready.gov/community-emergency-response-team

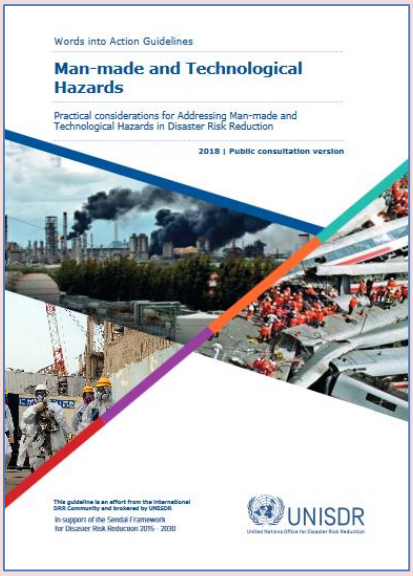
The Community Emergency Response Team (CERT) program educates volunteers about disaster preparedness for the hazards that may impact their area and trains them in basic disaster response skills, such as fire safety, light search and rescue, team organization, and disaster medical operations. CERT offers a consistent, nationwide approach to volunteer training and organization that professional responders can rely on during disaster situations, which allows them to focus on more complex tasks. Through CERT, the capabilities to prepare for, respond to and recover from disasters is built and enhanced.

Since 1993, CERT has impacted communities across the country, building essentials skills and capabilities to prepare for and respond to any disaster. There are now CERT programs in all 50 states, including many tribal nations and U.S. territories; each unique to its community but all essential to building a Culture of Preparedness.

The CERT program was designed as a grassroots initiative and specifically structured so that the local and state program managers have the flexibility to form their programs in the way that best suits their communities. CERT volunteers are trained to respond safely, responsibly, and effectively to emergency situations, but they can also support their communities during non-emergency events as well. There are over 2,700 local CERT programs nationwide, with more than 600,000 individuals trained since CERT became a national program.

FEMA's Community Emergency Response Team Program trains volunteers to prepare for the types of disasters that their community may face. Through hands-on practice and realistic exercises, CERT members:

Words into Action guideline: Man-made/ technological hazards



Source: https://www.unisdr.org/files/54012_manmadetechhazards.pdf

The Guide takes a practical approach in addressing man-made and technological hazards, and builds upon previous analyses and recommendations relating to such hazards in the context of DRR.

The Guide builds on the outcomes of the Open-ended Intergovernmental Expert Working Group on Indicators and Terminology for the Sendai Framework, and the work on hazard classification and terminology related to man-made hazards. It covers the following classes of hazards:

- Man-made (i.e., anthropogenic, or human-induced) hazards are defined as those "induced entirely or predominantly by human activities and choices". This term does not include the occurrence or risk of armed conflicts and other situations of social instability or tension which are subject to international humanitarian law and national legislation. Technological hazards are normally considered a subset of man-made hazards.
- Chemical, nuclear and radiological hazards, as well as transport hazards are defined as those "originate from technological or industrial conditions, dangerous procedures, infrastructure failures or specific human activities.

Examples include industrial pollution, ionizing radiation, toxic wastes, dam failures, transport accidents, factory explosions, fires and chemical spills. Technological hazards also may arise directly as a result of the impacts of a natural hazard event. A technological accident caused by a natural hazard is known as a Natech.

This guide does not cover structural collapses of buildings and infrastructures such as bridges, dams and factories as this is subject of another guide.

Public review of Words into Action guide on Man-made and Technological Hazards: Practical considerations for Addressing Man-made and Technological Hazards in Disaster Risk Reduction

As an effort from the international DRR Community and brokered by UNISDR, this official public consultation version is a product of a long and detailed process of drafting, consultation and review. This document will be on PreventionWeb for public review during 3 months and has the purpose to ensure we haven't overseen aspects that are important to consider. Share your comments through the survey here.

This Words in Action (WiA) Guide addresses man-made hazards, including the subset of technological hazards. The Guide takes a practical approach in addressing man-made and technological (Man-made and Tech hazards), and builds upon previous analyses and recommendations relating to such hazards in the context of DRR.

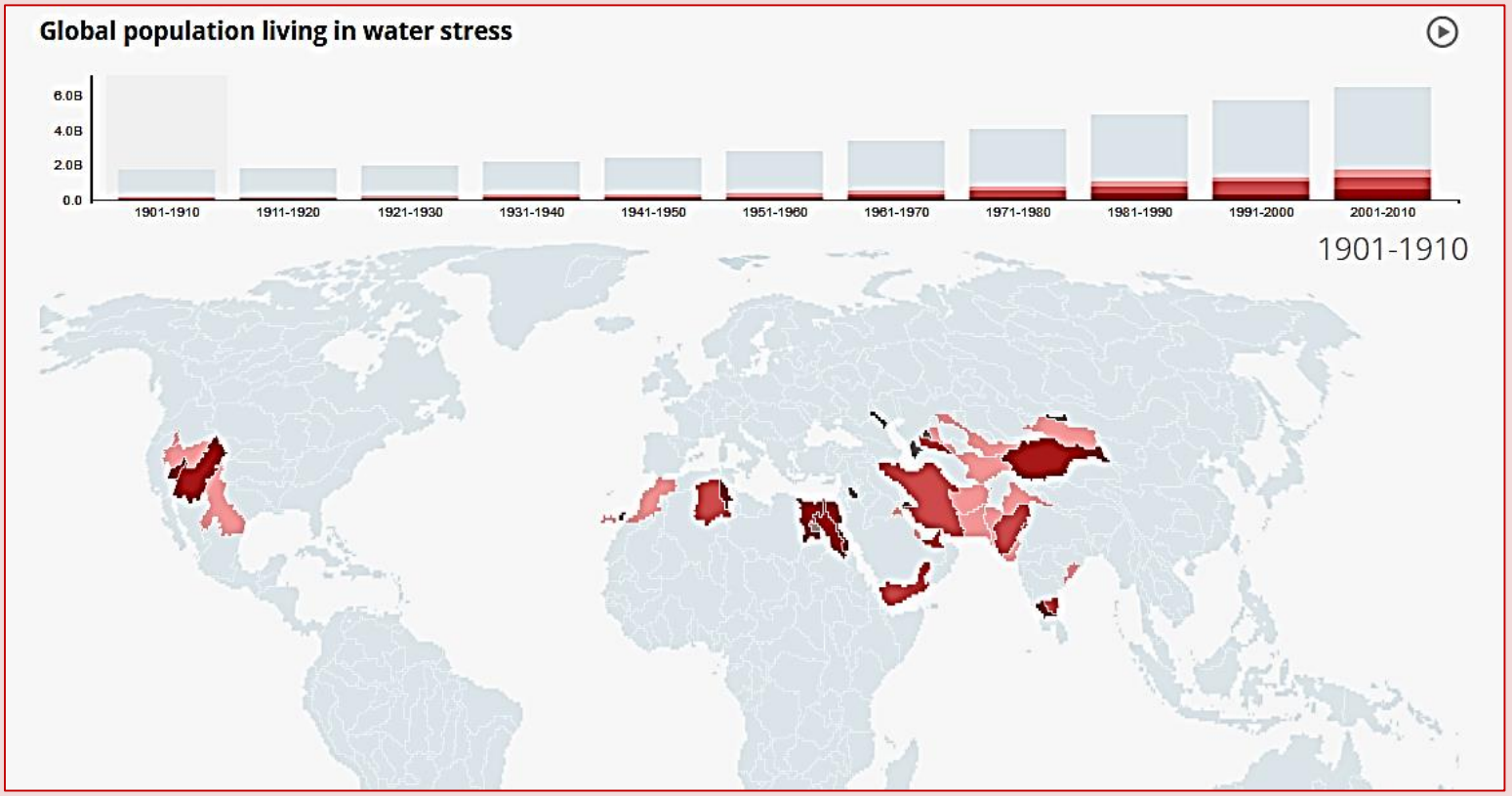

ICI
International
CBRNE
INSTITUTE
CBRNE-Terrorism Newsletter
W
O
M
D
C2BRNE
DIARY
ASYMMETRIC
THREATS

A dry future? New interactive map highlights water scarcity around the globe

Source: http://www.homelandsecuritynewswire.com/dr20181105-a-dry-future-new-interactive-map-highlights-water-scarcity-around-the-globe

Nov 05 – The average person in Europe uses 3,000−5,000 liters of water per day, of which the lion's share is spent on food production – a considerable part on the other side of the globe. The world's limited water resources are becoming an even more pressing issue as populations grow and climate change causes droughts in the global South and North. While studies have already provided a number of ways to reduce our consumption of water, this valuable information is often left unused.

Water researchers at Aalto University wanted to better communicate research findings to a broader audience. The Water Scarcity Atlas, a web application created by Postdoctoral Researcher Joseph



Guillaume and Assistant Professor Matti Kummu, uses interactive global maps to provide an introduction to the problems that arise with limited water – water scarcity – and ways to fight them.

"Choices that consumers make here in the North have an effect on the other side of the world. Understanding water scarcity and the impact of your actions is the first step to shaping the future. We wanted to create a capacity building tool so that people can better understand what makes their choices sustainable or not," explains Dr. Guillaume.

Aalto says that the atlas visualizes how water scarcity has evolved over the past 100 years and presents potential scenarios for the rest of this century. The user can explore how different factors such as changes in diet and food losses affect water resources all over the world.

"As water use increases, it becomes more difficult to access the resource sustainably. Eating less meat and avoiding food waste can reduce water use. We need to support initiatives by governments, NGOs, and companies with water stewardship programs. It's hard to strike a balance between environmental and human needs, especially when there isn't enough water to go around. We can work together to help farmers and other water users adopt new techniques, and establish effective management arrangements," says Dr. Guillaume.

The Water Scarcity Atlas is built on cutting-edge research. It is created in collaboration with the International Institute for Applied Systems Analysis (IIASA), which has contributed future

scenarios for household and industry water use. Aalto combined analyses of the potential for reducing water use, and global data on water use and availability, modelled by several research groups world-wide as part of the Inter-Sectoral Impact Model Intercomparison Project (ISIMIP).The visualizations were developed with Finnish startup company Lucify.

The Atlas also functions as a platform for researchers working on water scarcity at global scale. The Atlas features a publication database and a dataset database.

"We encourage researchers to contribute their own work to the Atlas. Most of the data exists in scattered journal articles. Our platform really allows anyone interested in global water scarcity to stay up to date on the latest research – in an accessible way."

Aalto says: "Which parts of the world suffer from water shortage and how can you help alleviate water scarcity? Explore the Water Scarcity Atlas: waterscarcityatlas.org."