

*Dedicated to Global First Responders*

# CBRNE

## NEWSLETTER



August 2017



[www.cbne-terrorism-newsletter.com](http://www.cbne-terrorism-newsletter.com)

IOI  
International  
**CBRNE**  
INSTITUTE



**DIRTY R-NEWS**



## Hawaii just released a guide for how to survive a nuclear attack amid high tensions with North Korea




Source: <https://dod.hawaii.gov/hiema/files/2017/07/HI-EMA-guidance-analysis-nuclear-detonation-JUN-2017-1.pdf>

July 24 – Hawaii's [Emergency Management Agency released](#) an ominous statement on how to survive and proceed in the event of a nuclear attack.

Citizens of Hawaii are advised to look out for emergency sirens, alerts, wireless notifications, or flashes of "brilliant white light" that will indicate that a nuclear detonation is incoming or underway.

From there, the agency instructs citizens to get indoors, stay indoors, and stay tuned via radio as "cell phone, television, radio and internet services will be severely disrupted or unavailable." Instead, expect only local radio stations to survive and function.

If indoors, citizens should avoid windows. If driving, citizens should pull off the road to allow emergency vehicles access to population centers. Once inside, Hawaiians should not leave home until instructed to or for two full weeks, as dangerous nuclear fallout could sicken or kill them.

Triggers	Mnemonic	Immediate Action	Rationale
Sirens sound <i>Attack-Warning</i> signal		<ol style="list-style-type: none"> <li>1. <u>If you are indoors</u>, stay indoors well away from windows.</li> <li>2. <u>If you are outdoors</u>, seek immediate shelter in a building preferably a concrete structure such as a commercial building or parking structure.</li> <li>3. <u>If you are driving</u>, pull safely to the side of the road and seek shelter in a nearby building or lie flat on the ground.</li> <li>4. DO NOT look at the flash of light.</li> </ol>	<ul style="list-style-type: none"> <li>Surviving the immediate effects of a nuclear detonation (blast, shock, thermal radiation, initial nuclear radiation) requires sheltering in resistant structures</li> <li>You may have only minutes to take protective action – take immediate action without delay</li> <li>There are no designated blast or fallout shelters in Hawaii</li> <li>Light generated by the weapon will damage unprotected eyes</li> </ul>
Emergency Alert System (EAS) advisory  Wireless Emergency Alert (WEA) system advisory		<ol style="list-style-type: none"> <li>1. Remain sheltered until you are told it is safe to leave or two weeks (14 days) have passed, whichever comes first.</li> <li>2. You may be advised that it is safe to leave your shelter for short periods of time to locate food, water and medical care.</li> <li>3. Electrical, water and other utilities may be severely disrupted or unavailable.</li> </ol>	<ul style="list-style-type: none"> <li>Following the detonation, sheltering from radioactive fallout for up to 14 days is critically important</li> <li>Public may need to briefly leave their shelters to locate essential supplies and equipment</li> <li>Emergency Management will assess residual radiation levels and advise when sheltering can be discontinued</li> </ul>
Brilliant white light (flash) is observed		<ol style="list-style-type: none"> <li>1. Listen to local AM-FM radio stations for official information.</li> <li>2. Cell phone, television, radio and internet services will be severely disrupted or unavailable.</li> <li>3. Small portable walkie-talkies may give you communication with nearby shelters.</li> </ol>	<ul style="list-style-type: none"> <li>Local AM-FM broadcast radio is most survivable and may be useful in advising the public post-detonation</li> <li>Other communication technologies may be damaged by weapons effects such as EMP<sup>1</sup></li> <li>FRS<sup>2</sup> and GMRS radios are widely available in the community and may be useful in keeping people in communication with one another</li> </ul>

<sup>1</sup> EMP = Electromagnetic Pulse

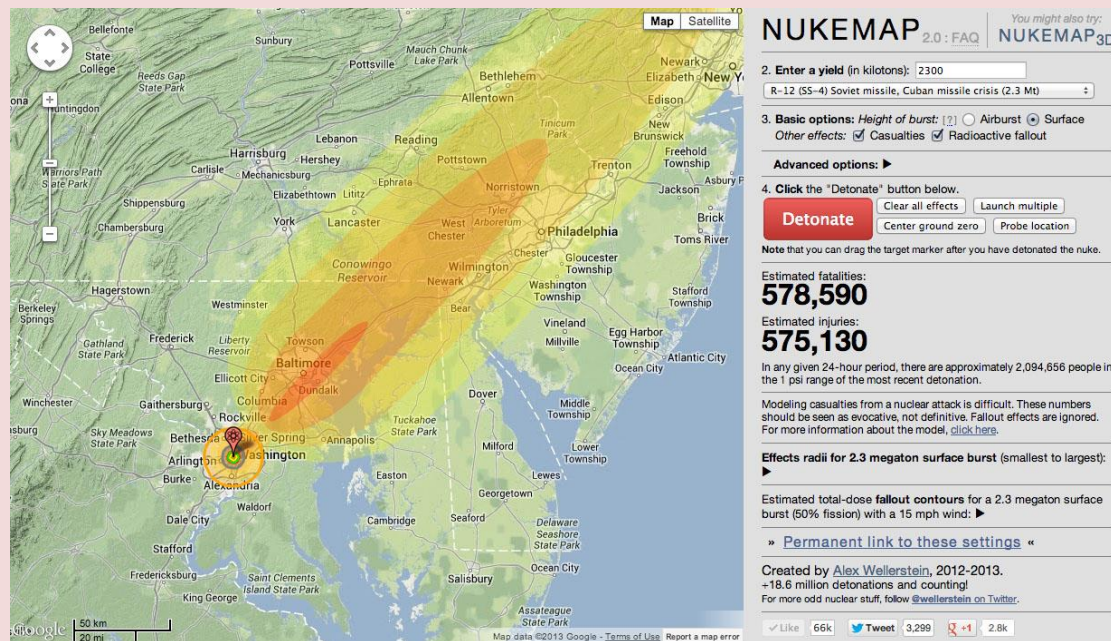
<sup>2</sup> FRS = Family Radio Service (unlicensed); GMRS = General Mobile Radio Service (licensed)



## NUKEMAP creator Alex Wellerstein puts nuclear risk on the radar

By Elisabeth Eaves

Source: <http://thebulletin.org/2017/july/nukemap-creator-alex-wellerstein-puts-nuclear-risk-radar10909>



In 2012, science historian Alex Wellerstein created NUKEMAP, an online tool that lets users pick a place, pick a type of nuclear weapon, and click a red button that says “detonate” to see the devastating results. By May of 2017, NUKEMAP had enabled about 113 million “detonations” by users all over the world. In this interview, Wellerstein talks to *Bulletin* contributing editor Elisabeth Eaves about why the tool is so popular, the need for better civil defense, how scientists can help change the culture, and much more. [Read this free-access interview in "After midnight," the July/August issue of the Bulletin's digital journal.](#)

## How to create realistic radiation scenarios for first responder training

By Steven Pike

Source: <http://www.argonelectronics.com/blog/how-to-create-realistic-scenarios-for-first-responder-training>



July 15 – The ability to project realism into [CBRN training](#) is an ongoing challenge for first responders. And especially so when it comes to the practical, hands-on use of highly specialist equipment such as radiation detectors.





**CBRNE-TERRORISM NEWSLETTER – August 2017**

When firefighter Ross Smallcombe was asked to provide the duty crew at the Ryde Fire Station on the Isle of Wight with a short training session on the use of their service's [Mirion](#) Rados RDS 200 Universal Survey Meter, he quickly realised that there were some significant gaps in the crew's practical hands-on experience of the device.

"The biggest problem I had was being able to carry out realistic first responder training that gave a real understanding and hands-on approach to radiation," says Smallcombe.

"After visiting the Argon website, I contacted them to enquire about the use of a [Rados RDS200 simulator](#). Within an hour I was having a conversation with Steven Pike (Managing Director) who was willing to assist me with my plans and loan me a kit which included simulation emitters (both directional and spherical), simulation powders and liquids, the [GMP-11-SIM simulation beta contamination probe](#) and [EPD-MK2-SIM](#) (personal dosimeters).

"This was fantastic news. Now I could plan a training package based on realistic scenarios, whilst evaluating this new equipment."

The opportunity to experience real-time radiation simulation technology through the use of the Rados RDS 200 SIM was to prove an invaluable learning tool for the Ryde Fire Station crew.

Smallcombe firstly stripped the subject back by preparing a lecture about the Rados RDS 200, its application within varied industries, what it detects, how to use it, its construction, etc.

He then created a second training session covering the basics of radiation including various types of radiation, dose rates, fire service procedures and a section covering Chernobyl and radiation levels around the disaster zone.

The two sessions were then followed by a short practical hands-on session using the Rados RDS 200 SIM and GMP-11-SIM beta contamination probe.

"The gamma simulation emitters were turned on and beta liquids and powders were used on food to enable the simulation detection equipment to show readings. This was the first time any of us had seen readings on the Rados RDS 200," says Smallcombe.

**First responder radiation training scenarios**

Using the RDS 200 simulator, Smallcombe was able to set up a series of realistic, scenario-based first responder training sessions which included:

- Simulating a road traffic collision involving radiation - This was set up to simulate a broken container with a source of radiation inside. Using a directional emitter, EPD-MK2- SIM (personal dosimeters) and RDS 200 SIM, a van was parked and a car was put into position to simulate a rear collision. The car contained a casualty that had leg entrapment. The challenge was to release the casualty and make the area as safe as possible while keeping crew exposure to a minimum
- Replicating a school laboratory accident - A series of buildings were set up to simulate the accidental spilling of a radioactive substance. The crew were tasked with rescuing the walking wounded, sourcing and containing the radioactive material and setting up a decontamination process.
- Locating a source of radiation - Radiation emitters were placed in various locations around the abandoned village and crews in pairs were sent off with the Rados RDS 200 SIM and EPD MK2 SIM. Their goal was to locate the source of the radiation, report back its precise location and to determine how close the team could safely get without exceeding the acceptable radiation dose rate.
- Simulating a casualty fleeing a scene - This scenario was designed to simulate a casualty covered with contaminant fleeing from the scene of a small radiation incident. Beta simulation radioactive contamination powder was placed on windowsills, handrails and flooring within the building. The crew's challenge was to identify and follow the trail to locate the lost casualty.
- Finding safe routes - A casualty was placed within a group of buildings and two radiation emitters were set up to simulate various strengths and direction of radiation. The task for the crew was to locate the casualty within the contaminated area and to map out a safe route through the building.

Simulation training accurately replicates how real devices respond to a range of chemical agents. Intelligent, computer-based simulation tools are offering first responder teams a safe, workable and cost-effective training opportunity.



**CBRNE-TERRORISM NEWSLETTER – August 2017**

Says Smallcombe, "The simulation kit enabled us to train in a very realistic and practical way and all crews that were able to be part of the training sessions are now confident and competent with the use of the RDS 200.

"Nothing can compare with realistic training in the fire and rescue service."

►► Read the [full case study](#) from Ross Smallcombe and the Ryde Fire Station

## The North Korea that can say no

By Bruce Cumings

Source: <http://thebulletin.org/north-korea-can-say-no9048>

Jan 2016 – Some years ago, I spoke with a former Soviet official who had worked in North Korea. He said that you could try to direct, cajole, or nudge the leadership to do something that, to a foreigner, looked to be in their best interests. They would smile, seem to nod assent, or might even say yes, then do the opposite—even when it directly contradicted their presumed interests. You can call it bloody-minded, self-centered, even pig-headed; they don't care. But this dogged insistence on going their own way is as much a part of North Korea's historic behavior pattern as it is a palpable obstacle to international cooperation—even with North Korea's close allies.

This trait might explain one of the real oddities in US-North Korean relations, which occurred back in the early months of the Obama administration. In the only burst of activism toward engaging the North in the past seven years, Washington brought to the table a package of proposals to revive the Six-Party talks, in return for a moratorium from North Korea on testing nuclear weapons or launching long-range missiles. A short time later, on April 5, 2009, the North sent a Taepodong-2 rocket into the stratosphere, where it tried but failed to put a satellite up. No American official could explain this odd sequence of events—at least publicly. They treated it as a direct stab in the back, ending any attempts at engagement, while the North said it had informed the Americans of the coming launch.

After this week's nuclear weapons test, it is China's turn to wonder about a knife in the back. The People's Republic of China (PRC) is North Korea's neighbor, and has for decades been its closest ally. Personal relationships among the top leaders of the two countries go back 80 years, when Kim Il Sung was part of a joint Korean-Chinese guerrilla war against Japan in Manchuria, and joined the Chinese Communist

Party. China saved North Korea from oblivion when it intervened in the Korean War in 1950.

But at least since the North's third nuclear test in February 2013, relations between the two countries have been unprecedentedly cold. After the tests, Chinese president Xi Jinping openly stated that Pyongyang's actions threatened world peace. Mister Xi has subsequently met several times with South Korean president Park Keun Hye, with whom he apparently has a warm friendship—and in a fit of pique, Pyongyang responded by blowing off several short- and medium-range missiles on the eve of Xi's visit to Seoul in July 2014.

In recent months, China has sought to warm up the relationship with the North. Last October, it sent Politburo Standing Committee member Liu Yunshan to North Korea's celebration in Pyongyang of the 70<sup>th</sup> anniversary of the founding of its Worker's Party. Liu was the highest-ranking visitor from the PRC in several years; he was seen waving from a podium with Kim Jong Un high above the central square, where millions had gathered for the event. [Some analysts thought that the quid pro quo for this visit was the North's pledge not to test A-bombs or long-range missiles](#), as Javier C. Hernandez wrote in the *New York Times*. In an act that seemingly supported this view, in December Kim Jong Un sent his favorite singing group—the Moranbong Band, consisting of 20 pretty young women in stylish Western garb—to Beijing for several performances. When it became clear that no high officials would show up for the gala opening, [the group was abruptly called home](#). It is likely that Beijing had picked up signs of the coming nuclear test; in any case, China condemned the test, and relations are back in a deep freeze.

On the surface, China's actions would seem to be a big problem for Pyongyang. Most of the goods available in North Korea's markets



**CBRNE-TERRORISM NEWSLETTER – August 2017**

are made in China. Pyongyang earns huge amounts of foreign exchange from Chinese firms exploiting its coal, metal, and mineral reserves (which are seemingly inexhaustible). The North's trade with China was estimated at more than \$6 billion in 2015, not counting informal or black market trade which is also assumed to be quite substantial.

On the diplomatic front, North Korea has also suffered from the Chinese response to its nuclear tests. China has also joined the United States and other countries in slapping United Nations sanctions on the North, and no doubt will do so again in the coming days. This is a major turn-about—for more than a decade, high American officials (especially Defense Secretary Donald Rumsfeld during the second Bush administration) have been hoping that Beijing would join with Washington to gang up on Pyongyang and maybe even end the Kim regime.

Such thinking assumes a uniform view in Beijing about North Korea. In fact China's leadership, and the general public, are quite split. Many hardliners in the military and the party like the North (and correspondingly hate the United States). Xi Jinping is really the first Chinese leader openly to denounce Pyongyang's provocations, whereas his predecessor, Hu Jintao, gave a secret speech in September 2004 in which [he lauded the North's closed political system](#) for its ability to keep out subversive Western ideas and practices. No Chinese leader wants South Korea, with 28,000 American troops on the ground, controlling the Yalu River

border. President Obama's consistent strategy toward South Korea and Japan has been to get them to jettison their historical grievances and unite with the United States in containing China's growing power in the region. Tensions in the East and South China seas, mostly caused by Chinese expansionism, have tended to unite various countries behind American policy. In this milieu, China has many reasons not to make an open break with North Korea.

The key irritant in Sino-North Korean relations is that with every A-bomb or missile test, Washington ramps up its deterrent efforts in Northeast Asia, sending carrier task forces into the Yellow Sea, routing B-2 and B-52 bombers to the Korean theater, and deploying ever more anti-ballistic missile batteries, which China sees as a threat to its older missiles, including its antiquated ICBMs.

In the end, the likely Chinese response to the North's so-called "H-bomb" test will be a lot of hot air, more toothless or ineffective sanctions, and no serious break in Sino-Korean relations. There will be a continuation of the status quo between the two countries, while Pyongyang builds an ever more effective arsenal of bombs and missiles. North Korea's obstreperous behavior, so exasperating to foreign powers, might also be seen as a Game Theory 101 strategy by a small country surrounded by bigger powers who, when all is said and done, really don't like their smaller neighbor. Roar loudly, beat your chest, threaten all manner of mayhem, and recall Muhammad Ali's maxim: "I don't have to be who you want me to be."

*Bruce Cumings teaches in the history department of the University of Chicago, where he is the Gustavus F. and Ann M. Swift distinguished service professor. He is the author of [The Korean War](#), published by Random House in 2010. Cumings first became interested in the region while serving in the Peace Corps in South Korea in 1967. He was also the principal historical consultant for the Thames Television/PBS six-hour-long documentary [Korea: The Unknown War](#).*

## The Terrible Magic of Atomic Weapons

By George Friedman

Source: <https://geopoliticalfutures.com/terrible-magic-atomic-weapons/>

Aug 02 – It's hard to build a national policy on the assumption that these weapons moderate the depraved. On Aug. 6, 1945, the United States dropped an atomic bomb on Hiroshima. The U.S. remains the only country to have ever used nuclear weapons. As part of our project to review major World War II battles, I will examine the reasoning on both sides that led to the use of this weapon.

The Japanese had entered the war because of the effectiveness of U.S. economic sanctions imposed after the Japanese had invaded Indochina. As an industrial power devoid of its own





## CBRNE-TERRORISM NEWSLETTER – August 2017

resources, Japan had to import nearly all of its resources, mostly from Indochina and the Dutch East Indies.

The United States feared that Japan, after dominating the Western Pacific, would soon threaten its interests in the central and eastern Pacific. Japan had treaty agreements with France and the Netherlands guaranteeing shipments of commodities. When both were overrun by Germany, it became uncertain who would control their Pacific colonies, and Japan could not live with that uncertainty. When the U.S. tried to restrict Japan's access to certain resources in order to limit Japanese expansion, Japan had a choice: It could continue expanding and face war with the United States, or it could allow itself to become completely dependent on the United States for access to minerals.

The United States saw Japan as an international outlaw that needed to be heeled by peaceful sanctions. The Japanese saw the United States as using sanctions to crush Japan's economy. The result was war.



### U.S. and Japanese Goals

The United States had two strategic goals. The first was to disrupt Japanese access to Southeast Asia supplies without invading the Dutch East Indies or Indochina. This meant intense submarine warfare. The second goal was to bring itself into range of Japan so that it could conduct a strategic bombing campaign. By 1945, the submarine campaign had dramatically reduced the flow of supplies, and the capture of Saipan and Tinian had brought B-29s within range of Japan.

The Japanese strategy strategic goal in 1945 was to prevent the occupation of the Japanese homeland and retain the existing regime, particularly the position of the emperor. The primary strategy for this was to create a defensive system that would potentially impose unacceptable casualties on the United States.



During the Pacific campaigns, the Japanese had learned that American pre-invasion bombing and bombardment were of limited value. The U.S. succeeded by forcing land battles that had high casualty rates but low casualty totals, relative to other battles in World War II, since these battles were comparatively small. This worked in the Gilberts, the Marianas and the Marshalls. What this proved, however, was that the U.S. would incur a high casualty rate in an invasion of Japan, which would require a substantially larger force.

The U.S. Navy suffered the greatest casualties due to the kamikazes. The Japanese strategy therefore focused on using the kamikazes to attack the Navy and on forcing battles of attrition





**CBRNE-TERRORISM NEWSLETTER – August 2017**

by layering forces, including civilians, into the interior. Although this imposed catastrophic casualties on the Japanese – estimates say a quarter million died in Okinawa – American troops also suffered severe casualties.

The Japanese were betting on asymmetry of interest. They were fighting for their homeland and for a regime that was far from delegitimized. The Americans were fighting for an increasingly marginal goal – dismantling the Japanese regime. The Japanese believed that the U.S. would give up first and agree to a truce rather than requiring Japan's unconditional surrender.

This was a reasonable assumption given that the United States' most experienced troops were already exhausted from war in North Africa, Italy, France and Germany, and its most seasoned Marines had been fighting since Guadalcanal. If the U.S. did invade Japan, the troops that would be sent were the draftees from 1944 and 1945 who were inexperienced and not yet blooded. Instead, the U.S. hoped that bombing and submarine warfare would have forced capitulation.

It hadn't. Most cities were devastated, and the condition of the economy had reduced the country to penury. But the Japanese wouldn't capitulate. While they did send out peace feelers, they didn't include an offer to surrender – merely an offer to negotiate a settlement. The agreement among the Allies was that only unconditional surrender was acceptable, since the U.S. did not want a repeat of Versailles after World War I. They wanted to end Japanese expansion, and a prolonged negotiation would have exacerbated the ongoing bloodshed in China. Besides, Japan had already lost credibility with respect to peace negotiations, as it had previously been engaged in such talks while its fleet was preparing for Pearl Harbor. The argument for a negotiated settlement was not nearly as obvious then as it is now.

**The Atomic Project**

Still, the U.S. was caught in a bind. It couldn't afford the potential costs of invading, and it also couldn't accept anything less than total capitulation, which the Japanese weren't willing to offer. It was this strategic situation that led to the use of atomic bombs. The atomic project was driven by German scientists and those who feared that Germany would develop a nuclear weapon. But the Germans didn't have the resources necessary to both define the concept and create the weapon; only the U.S. was capable of such a massive undertaking during the war. But the Americans were unaware of the limitations of the German program and therefore launched the Manhattan Project, the U.S. program to develop an atomic bomb.

Years later, some would argue that the United States dropped the bomb to frighten the Soviets or keep them out of Japan. But the Soviets couldn't have invaded Japan anyway; they lacked the capability to send a massive number of troops there. The Soviets, moreover, already knew about the bomb, although the U.S. didn't realize that at the time. If the U.S. wanted to impress the Soviets, it had many ways to do it that didn't involve bombing Hiroshima and Nagasaki.



A boy floats a candle-lit paper lantern on the river in front of the Atomic Bomb Dome during 70th anniversary activities, commemorating the atomic bombing of Hiroshima on Aug. 6, 2015. Photo by Chris McGrath/Getty Images



**CBRNE-TERRORISM NEWSLETTER – August 2017**

The first test of the bomb took place in July 1945, in the midst of the American strategic conundrum. Would the country accept the cost of occupying Japan when it would turn out that there was a potential alternative to massive American casualties? It's unclear what Harry Truman would have done if the bomb wasn't an option, but he would have been pilloried had he invaded or had he not. The country, the troops included, was tired of war and wasn't willing to pay the cost of invasion. But a peace treaty that allowed the Japanese regime to stay intact would have left the fundamental issues that started the war unsettled. This is not an argument as to which side was more just. It is simply to say that a peace treaty wouldn't have been a conclusive end to the war.

It was clear that the Japanese leadership was prepared to accept the destruction of cities, and that the population was not prepared to rise against the regime. The Americans therefore believed that the Japanese were not prepared to surrender, which in retrospect was true. The Japanese view was that the U.S. either wouldn't invade or, if it did, would face casualties that would cause it to accept a peace treaty. But the atomic bomb presented another potential scenario. Although Japanese cities had faced devastating attacks before, this threat was different because a single bomb could do the damage of a thousand. Moreover, the extent of the casualties from an atomic bomb was still unclear, in part due to the uncertainty of injury caused by nuclear fallout. But the Americans were focused on the psychological effect it would have. While the Bombing of Tokyo had a devastating impact, the means of death was not a mystery.

The atomic bomb worked terrible magic. The suddenness and totality of the strike created a unique sense of helplessness. It was instantaneous, and it came from nowhere. There were some in the pro-war faction who argued that the bomb used on Hiroshima was simply another massive air attack and not a new weapon. The deaths and destruction were, from their point of view, bearable because it was part of a known pattern.

They refused to surrender. Some even attempted a coup, which came close to success. But for some leaders, Hiroshima immediately tipped the balance to surrender. But capitulation only came after Nagasaki and after the U.S. acknowledged that the emperor would remain as a figurehead, causing him to shift his position.

Ultimately, the atomic bomb ended the war, partly because of the psychological shock and partly because Japan realized that the bomb could be used against Japanese defensive forces massed to face a potential invasion. We can only speculate how many American casualties or how many more Chinese casualties this move prevented.

**A Sobering Effect**

Eight other nations have acquired nuclear weapons: the United Kingdom, the Soviet Union, France, China, Israel, India, Pakistan and South Africa. (South Africa has subsequently given up these weapons.) North Korea has developed nuclear devices but it's unclear whether it has a deliverable nuclear weapon. None of these countries has used their weapons, though some have found themselves in circumstances where using them would have made sense. Some, particularly Mao's China, raved about what they would do with nuclear weapons once they had them. But they didn't end up doing what they said they would do. In a sense, they aren't weapons designed to fight armies. (Tactical nukes might be an exception, although they have also not been used.) They seem to have a sobering effect.

The question today is whether the magic of these weapons might sober [North Korea or Iran](#). Some argue that it would sober North Korea, the more immediate and more important case. Human history, and specifically the 20th century, are filled with nations that committed acts of political depravity – but not, even in the case of Stalin or Mao, nuclear depravity. The problem is that it's hard to build a national policy on the assumption that nuclear weapons moderate the depraved.

In making the decision to use a nuclear weapon, the U.S. faced some tough choices. It had to balance its moral responsibility to American troops and those who were still being slaughtered by the Japanese against the lives of those who would be killed in a nuclear attack. But the idea that Japan was ready to surrender is a myth. It was ready to negotiate a peace deal; it wouldn't accept unconditional surrender. This could have opened the door to another war, allowing the slaughter of Americans who had already fought and survived a long war.

But it did deeply sober the United States. [It opened an abyss](#) the U.S. and all the other nuclear powers looked into and recoiled from. Their use may well have prevented a global nuclear war between the U.S. and the Soviet Union. But will the sobering effect of nuclear





weapons extend to other countries like North Korea? Or will a nuclear North Korea embrace the abyss? This is not a geopolitical question as much as a psychological one.

## Badly packaged nuclear consignment on plane to Brussels

Source: <http://deredactie.be/cm/vrtnieuws.english/News/1.3035577>

July 30 – Passengers on flights between Cairo, Zürich and Zürich to Brussels could have been exposed to radiation without realising it. The incident happened on the 13 July when a used radioactive source destined for a company in Fleurus (Hainaut) was transported on the plane without sufficient protective packaging.

When the package arrived at NTP Radioscopes in Fleurus, the company reported what had happened to the nuclear watchdog FANC and an investigation was launched.



NTP Radioscopes produces radioactive sources that are used in, for example, industrial imaging. Last Tuesday the company received a package containing a consignment of a used iridium 192 source that had been sent from Egypt. The package had been stored in a hangar at Zaventem Airport since

it had been flown over.

A member of staff's radiometer registered excess levels of radioactivity and the nuclear watchdog FANC was brought in to investigate. It found that the source was not packaged and labelled correctly and that the package should not have been sent in that state. The sender of the package will now be contacted. The source gave off radiation levels of 2 mSv/hour. The annual radiation exposure limit in Belgium is 1 mSv, in addition to exposure to 2.8 mSv/year natural radiation.

"Not a life-threatening dose"

As the package was transported on 2 flights FANC calculated the maximum radiation dosage passengers could have been exposed to. This is reported to be a conservative estimate as it is not known where the packed was in the planes' cargo holds.

A FANC spokesman told VRT News that "The maximum dose to which a passenger that was sat above the package on the Cairo to Zürich flight was 6.6 mSv. This is 3.1 mSv for passengers on the Zürich-Brussels flight".

"As regards exposure, this is between 5 and 6 times more than the limit, but people shouldn't be alarmed. This is not a life-threatening dose.

FANC has ranked the incident as a 2 on the International Nuclear Event Scale (INES). INES has 7 levels ranging from 1 (anomaly) to 7 (serious accident).

## Survival under atomic attack (1950)

Source: <https://www.orau.org/ptp/Library/cdv/Survival%20Under%20Atomic%20Attack.pdf>

## 4 Frightening Ways North Korea's Nuclear Weapons May Actually Be Used

By Francis Grice

Source: <http://nationalinterest.org/feature/4-ways-north-koreas-nukes-may-actually-be-used-21790>

Aug 05 – Kim Jong-un has been at it again: another intercontinental ballistic missile [test](#) and a further [verbal threat](#) against the United States. Yet, despite all of North Korea's technical



**CBRNE-TERRORISM NEWSLETTER – August 2017**

developments and rhetorical bluster, the United States and its allies are almost certainly safe from a deliberate nuclear strike. Kim Jong-un is a [rational actor driven](#) by one all-consuming goal: survival. To intentionally attack the United States or its allies with nuclear missiles would almost certainly result in nuclear retaliation or a regime-change driven invasion. As Robert Kelly noted in the [National Interest](#), “Pyongyang knows there is no way to use their weapons for gain that would not immediately provoke massive counter-costs.”

This does not mean, however, that the world is entirely safe from a North Korean nuclear attack. There are at least four scenarios that could lead to the pariah state’s nuclear weapons being used: foreign invasion, domestic uprising, nuclear accidents, or acquisition by terrorists.

**Scenario One: Foreign Invasion**

The high-costs versus low-reward calculus that currently holds Kim Jong-un back from using his nuclear weapons could change if the Trump administration responded to North Korea’s ongoing [missile provocations](#), nuclear threats and abhorrent [human-rights record](#) with a major military intervention. In that situation, Kim could feel sufficiently certain that his regime was destined for collapse and his own life forfeit that he decides to use nuclear weapons. These might be deployed against the invaders as a weapon of last resort—hoping to destroy either their material means or political will—or as a final act of vengeance against their homelands. It is difficult to gauge whether Kim would act in this way because in the two most recent interventions—America’s overthrow of Saddam Hussein in Iraq and NATO’s push to depose Muammar Gaddafi in Libya—the regimes in question had abandoned their Weapons of Mass Destruction some years earlier. Would either dictator have used nuclear weapons as a last-ditch survival attempt or as revenge for their imminent demise had they possessed them? We will never know.

To gain a better understanding, we must reach back in time to the end of World War II, when Adolf Hitler ordered vast swathes of Nazi occupied territory to be destroyed (albeit using conventional methods) once it became clear that his forces were all but defeated. He issued two famous orders: that Paris be turned “[into a pile of Rubble](#)” and Warsaw be “[levelled to the ground](#).” Hitler thought that this would impede allied progress as a [scorched-earth strategy](#) and help to stamp out all partisan resistance against the German occupiers. He also [wanted to deprive](#) the world of these two cities on the basis that if Germany could not have the cities, no one else should have them. At the same time, Hitler felt able to disregard the risk of retaliation from the allies in response to these atrocities because they were already engaged in a total war with the Nazi regime.

In Paris, the unthinkable never happened because the general assigned to carry out the command—Dietrich von Choltitz—was not a member of the Nazi party and had come to believe that Hitler was [sufficiently insane](#) that this order should be ignored (although von Choltitz was scarcely a saint—he had previously destroyed other population hubs). Tragically, in Warsaw, the task was assigned to the ideologically fervent and high-ranking SS Officer, Erich von dem Bach-Zelewski, who executed his task with horrifying brutality and razed Warsaw to the ground, killing [150,000–180,000 people](#). Unfortunately, the political indoctrination and subordination of the armed forces to the regime in North Korea means that the commanders to whom Kim Jong-un would issue his nuclear attack orders would be more likely to be party loyalists like Bach-Zelewski than more independent thinkers like von Choltitz.

**Scenario Two: Domestic Uprising**

The rationality calculus facing Kim Jong-un could also change as a result of domestic rebellion within North Korea. The extreme security measures employed by the regime makes an uprising [extremely improbable](#), but in the unlikely event that one did erupt and it was winning, Kim Jong-un might find himself staring over the abyss. He could then decide that threat was sufficiently pressing that nuclear weapons should be used, either against the rebels themselves or any outside allies who were supplying aid and support.

Although no state has ever used nuclear weapons to suppress internal dissent, other weapons of mass destruction have been employed for this purpose. Saddam Hussein, for example, used chemical weapons against his own people when facing significant threats against his rule in [1988](#) and again in [1991](#). More recently, in the ongoing Syrian Civil War, Bashar al-Assad has deployed chemical





**CBRNE-TERRORISM NEWSLETTER – August 2017**

weapons in rebel held areas on [numerous occasions](#). The notion that the even more fanatical regime of Kim Jong-un might be willing to use nuclear weapons against his own population or outside supporters of a rebellion, if his regime appeared to be similarly tottering on the brink of collapse, is not at all far-fetched.

**Scenario Three: Nuclear Accident**

Alternatively, North Korea might launch or detonate a nuclear weapon unintentionally. The comparatively short lifespan of the country's nuclear program, along with its relative isolation from the expertise of other nuclear powers, means that its nuclear safety measures are likely to be [dangerously under developed](#). This increases the chance that a nuclear missile could be fired or a warhead detonated involuntarily as a result of a hardware failure or software errors. To make matters worse, the regime seems to be in a colossal hurry to increase the size of its stockpiles of nuclear weapons and ballistic missiles. This is a problem because when states place a premium upon expanding their nuclear arsenals at all costs, it may come at the cost of making [parallel advances](#) in nuclear and missile safety. Unless North Korea slows down the current pace of its weapons-enlargement efforts to ensure that it is developing equivalent safety systems, the warheads and missiles that it produces could be accidents just waiting to happen.

Another challenge is the potential for North Korea's early warning systems to misread the presence of harmless artifacts in its airspace as being an inbound nuclear missile and reacting with a nuclear response. Even the most developed and experienced of nuclear powers have faced this challenge and only survived due to the good judgement, immense courage, and risk-taking of key individuals. One example happened in 1983, when Soviet Lt. Col. Stanislav Yevgrafovich Petrov identified what appeared to be five inbound [intercontinental ballistic missiles](#) hurtling towards the Soviet Union. Under intense pressure, Petrov decided that the reading must be incorrect because if the United States was really attacking, he would expect to see hundreds of missiles rather than [just five](#). He was proved right, but the strain proved immense, leading him to later retire from the armed forces and suffer [a nervous breakdown](#). Had a less critically minded or a more ideologically zealous person been in charge, they might have told their superiors that

[a nuclear attack](#) was imminent and advised retaliation. In North Korea, the [totalitarian](#) nature of the regime increases the probability that the people staffing the early warning systems will interpret what they see on their screens literally—and without Petrov's critical eye. This could lead North Korea to fire nuclear missiles against a purely imagined attack. This risk is heightened by the paranoia of the regime about the outside world, which has led its nuclear weapons to be placed permanently on high alert and which further piles on the pressure for everyone involved. This makes an accidental nuclear weapon launch [even more likely](#).

**Scenario Four: Acquisition by Terrorists**

Finally, North Korean nuclear weapons could be obtained by one or more terrorist groups. The Kim Jong-un regime is already a major [black-market seller](#) of conventional weapons, missile materials and nuclear technology, and it would not be a huge leap for it to begin peddling fully functional nuclear bombs to the highest bidder as well, which could potentially include terrorist groups. This could happen if North Korean endured a fresh bout of unexpected economic turmoil or agricultural distress and the regime opted to sell its way out of the problem. Alternatively, the weapons could end up in the hands of terrorists by being stolen and smuggled out of the country. The risk of this happening was highlighted in the Nuclear Threat Initiative's 2016 Nuclear Security Index Report, which gave North Korea [a dismal score](#) of just thirty-eight out of one hundred for the security it provides against potential theft of its nuclear weapons when they are being used, stored or transported. An American military strike to disable North Korea's nuclear facilities could actually backfire because it might damage the existing security infrastructure around one or more of North Korea's nuclear storage facilities, which could make them easier to steal until they are repaired.

The acquisition of North Korean nuclear weapons by a terrorist group would be alarming because rationality in these groups is often lower and more complex than with state actors, allowing them to act with fewer constraints. One historical example of an at least partially irrational terrorist group was Aum Shinrikyo, whose leaders and followers genuinely believed that [Armageddon was coming](#) and that they needed to [strike against their](#)



[enemies](#) with weapons of mass destruction to achieve salvation. The cult's members did not fear nuclear retaliation because they believed that the end of the world was imminent anyway. They used biological and chemical weapons, but had been [eager to acquire](#) nuclear weapons and would likely have employed these as well if they could. Moreover, it is notoriously difficult to deter even rationally acting terrorists because they often operate in highly [diffuse networks](#) that are hard to track and difficult to destroy, they are usually [highly mobile](#), and typically do not have a [fixed territory](#) in the same way that state governments do. Ultimately, if a terrorist group was to successfully obtain a nuclear weapon from North Korea, it is not at all improbable that they might use it.

### Implications

The cold reality for the United States is that North Korea has nuclear weapons and that, despite the [defensive intention](#) of its government, they could end up being used in a number of scenarios.

Difficult though it may be to accept, the best path for the United States might be to recognize that North Korea is a nuclear power and begin working with it to try to reduce the likelihood of these scenarios coming to fruition. This could

involve guaranteeing to Kim Jong-un that the United States will neither invade North Korea nor actively support any internal or external dissident groups who are working to bring down the regime. It could also involve trying to work with the pariah state, either through China and Russia as intermediaries, to increase the quality of its safeguards against nuclear accidents and protections against nuclear theft. Helping the country to boost its economy through legal rather than illegal means would also reduce the risk that the regime might sell its weapons to terrorist groups if it experienced a sudden economic downturn or natural disaster.

[The recent statement](#) by U.S. Secretary of State Rex Tillerson to Kim Jong-un that "We do not seek a regime change, we do not seek a collapse of the regime, we do not seek an accelerated reunification of the peninsula, we do not seek an excuse to send our military north of the Thirty-Eighth Parallel . . . we are not your enemy, we are not your threat" may be a step in the right direction. Instead of living in denial about North Korea being a nuclear power, the United States could focus its efforts on helping the country to grow into a more stable, safe and secure nuclear power, so that its nuclear weapons pose less of a threat to the world.

*Francis Grice is an assistant professor of political science and international studies at McDaniel College in Maryland. He has a Ph.D. in defence studies from King's College London (2014) and recently co-edited the [Palgrave Handbook of Global Counterterrorism Policy and the Future of U.S. Warfare](#). He specializes in Asian Security Studies and International Relations.*

## Mexican Authorities Find Stolen Container With Radioactive Materials - Official

Source: <https://sputniknews.com/latam/201708031056137498-mexico-radioactive-materials-theft/>

Aug 03 – Mexican authorities have found and safely stored a stolen container containing radioactive materials, National Coordinator for Civil Defense Luis Felipe Puente said on Thursday.



National Coordinator for Civil Defense Luis Felipe Puente said on Thursday.

"The container with a radioactive source was found in the state of Nuevo Leon. It has been confirmed that the stolen radioactive source is in a safe place... there is no risk for the population," the official wrote on his Twitter page.

The theft of the container was announced on Wednesday by the country's Interior Ministry, which declared an alert in the states of Nuevo Leon, Coahuila, Zacatecas, Tamaulipas and San Luis Potosi.





Mexico has already faced a number of crimes related to radioactive materials, with the most recent case recorded in February and April of this year. In April 2013, a container containing the cobalt-60 isotope was stolen, while in three separate cases in 2014, 2015 and 2016, criminals stole iridium isotopes. All radioactive materials were eventually found, with even one the incidents resulting in the thieves' hospitalization.

## Trump threatens North Korea after US assesses they have miniaturized a nuclear warhead

Source: <http://edition.cnn.com/2017/08/08/politics/north-korea-missile-ready-nuclear-weapons/index.html>

Aug 09 – **President Donald Trump issued an extraordinary ultimatum to North Korea on Tuesday warning Pyongyang not to make any more threats against the United States or they will "face fire and fury like the world has never seen,"** during a photo op at the Trump National Golf Club in Bedminster, New Jersey.

"North Korea best not make any more threats to the United States. They will be met with fire and fury like the world has never seen... he has been very threatening beyond a normal state. They will be met with fire, fury and frankly power the likes of which this world has never seen before," he said.

Trump's harsh words come as US intelligence analysts have assessed that North Korea has produced a miniaturized nuclear warhead, according to multiple sources familiar with the analysis of North Korea's missile and nuclear program.

### Why North Korea wants nukes and missiles

*North Korea has long maintained it wants nuclear weapons and long-range missiles in order to deter the United States from attempting to overthrow the regime of Kim Jong Un.*

*Pyongyang looks at states like Iraq -- where former dictator Saddam Hussein was overthrown by the United States, and Libya -- the country's late leader, Moammar Gaddafi, gave up his nuclear ambitions for sanctions relief and aid, only to be toppled and killed after the US intervened in the country's civil unrest -- and believes that only being able to threaten the US homeland with a retaliatory nuclear strike can stop American military intervention.*

It is not believed that the capability has been tested, according to the sources.

This is not a consensus view from the entire intelligence community, one US official said. [The Washington Post](#), which was first to publish details, reported that it was the analysis of the Defense Intelligence Agency.

The US official familiar with the analysis of North Korea's missile and nuclear program says, in reference to North Korea's leader Kim Jong Un's boasts about the program, "we have to take him at his word and we need to be prepared to deal with it."

This official said the 'assessment' is continuing to be refined and updated as more intelligence is collected.

That language echoes comments made by Adm. Harry Harris, the head of the US Pacific Command (PACOM), during [a June speech in Australia](#).

"I know there's some debate about the miniaturization advancements made by Pyongyang. But PACOM must be prepared to fight tonight, so I take him at his word. I must assume his claims are true -- I know his aspirations certainly are," he said.

The officials all note that the evidence shows North Korea is making progress and the question is more about when not if North Korea is capable of launching a nuclear capable missile.

Referring to Kim Jong Un, the official said this report needs to be taken seriously as "we've seen him moving forward" on the program with no indication he is turning back.

US military commanders have long planned on the assumption that North Korea has a warhead and Pyongyang claimed to be able to miniaturize nuclear weapons in 2015.

In 2014, then-commander of US Forces Korea Gen. Curtis Scaparrotti said he believed that they had the capability to miniaturize a warhead. "I believe they have the capability to have miniaturized a device at this point, and they have the technology to potentially actually deliver what they say they have," Scaparrotti said at the time.

The Washington Post first reported details of the assessment on Tuesday just hours after North Korea threatened 'physical action'



**CBRNE-TERRORISM NEWSLETTER – August 2017**

in response to punitive sanctions unanimously passed by the United Nations Security Council over the weekend.

CNN has previously reported that US intelligence estimates Pyongyang may have the capacity to deliver a nuclear weapon to the US mainland by early next year and its missile program showed significant progress during two intercontinental ballistic missile tests in July.

"Assuming everything is true, including that intelligence assessment both existing and everything being accurate, there are still important unknowns," Republican Rep. Lee Zeldin told CNN's Wolf Blitzer, noting that questions still linger about whether a possible North Korean warhead could survive re-entry from the earth's upper atmosphere.

However, Zeldin also said that reporting of the development "increases the urgency of the time sensitivity" of efforts being taken by the US and its international partners to address North Korea's missile and nuclear programs diplomatically.

Earlier on Tuesday, President Trump was quick to highlight his administration's success in leading the UN Security Council to unanimously pass sanctions on North Korea.

"After many years of failure, countries are coming together to finally address the dangers posed by North Korea. We must be tough & decisive!" Trump wrote in a tweet on Tuesday morning.

But reports that North Korea has taken another big step forward in realizing its nuclear ambitions will likely only escalate an already tense situation after the latest chapter of rhetorical chest-thumping.

US Ambassador to the United Nations Nikki Haley called newly approved sanctions on North Korea "a gut punch" and warned of possible military action should the regime continue its aggressive actions.

Those military options include launching a "preventative war" against North Korea, according to White House national security adviser H.R. McMaster.

"If they had nuclear weapons that can threaten the United States, it's intolerable from the President's perspective. Of course, we have to provide all options to do that, and that includes a military option," McMaster said in an interview with MSNBC on Saturday.

Potential for miscalculation

Asked to expand on Trump's comments about North Korea on Tuesday, White House senior

counselor Kellyanne Conway described the remarks as "strong and obvious."

Trump's fiery rhetoric, however, plays into a long-standing North Korean narrative that the nation is under the imminent threat of invasion by the United States.

For decades, the North Korean regime has told its citizens that the United States is preparing for another war on the Korean Peninsula.

While nearly all historians say the north invaded the south, North Korea tells its citizens that the Americans actually started the war.

Regular military exercises between the US and South Korea enrage Pyongyang and are conveyed to citizens as further 'proof' of an American dress rehearsal for the next invasion. It is this narrative that the regime uses to justify the economic hardship and isolation that North Korean citizens have endured, in part due to their nation's ballistic missile and nuclear tests. Citizens are told they have to "tighten their belts" to protect their national sovereignty.

While both the US and North Korea have frequently used strong rhetoric as a strategic messaging tool, analysts warn that verbal escalations pose the risk of causing a catastrophic miscalculation.

"Complicating this delicate game is that we have two inexperienced, impulsive presidents in control of these massive military machines," Joe Cirincione, president of Ploughshares Fund, a global security foundation, told CNN on Monday. "It's one thing to make a mistake intentionally, it's another thing to stumble into a conflict, to make a move that you think is going to signal something to your opponent that triggers exactly the opposite," he added.

"So either one -- Kim Jong Un or Donald Trump -- could miscalculate and let loose a war unlike anything we have seen since World War II."

Is diplomacy still an option?

The risks of a military strike or all out conflict with North Korea are well documented and US Defense Secretary James Mattis has consistently said he favors finding a diplomatic solution -- warning earlier this year that military action could result in tragedy "on an unbelievable scale."

North Korean Foreign Minister Ri Yong Ho said over the weekend that Pyongyang "will, under no circumstances, put the nukes and ballistic rockets on the negotiating table," and would "teach the US a severe lesson" if it



**CBRNE-TERRORISM NEWSLETTER – August 2017**

used military force against North Korea.

But while that precondition appears to remain a non-starter for North Korea, Deputy Secretary of State John Sullivan told reporters on Tuesday that the US has made clear it will not talk to North Korea until it commits to stopping its missile and nuclear tests.

"We are not going to negotiate our way to the negotiating table," Sullivan said, noting that the view of his boss, Secretary of State Rex Tillerson has not changed since he took his first trip earlier this year Tokyo, Seoul and Beijing.

"When he talks about being willing to talk to the North Koreans and reassure them their peace and prosperity is best served by being engaged with us and having a denuclearized North Korean peninsula, it's on the assumption that the North Koreans stop their missile tests and stop their nuke tests and stop their development of nuclear weapons. So there is no deviation from those conditions," Sullivan said.

"We are not going to come to the table until the North Koreans have committed to that," he added.

North Korea was estimated to have between 13 and 30 nuclear weapons at the end of 2016, according to the Institute for Science and International Security -- noting that North Korea keeps secret the number of nuclear weapons that it has built, and there is little, if any, reliable public information about this value.

**N Korea's response**

North Korea's military is ["examining the operational plan" to strike areas around Guam](#) with medium-to-long-range strategic ballistic missiles, state-run news agency KCNA said early Wednesday local time.

The threat comes just hours after US President Donald Trump warned Pyongyang that if they continued to threaten the US, they would "face fire and fury like the world has never seen." Dubbed the "Tip of the Spear," Guam is a key to the US military's forward deployed presence in the Pacific and is home to thousands of American service members and their families.



The news comes as [Americans have grown increasingly concerned that North Korea poses a very serious threat to the United States, according to a new CNN Poll conducted by SSRS.](#)

Almost two-thirds of those polled, 62%, say Kim Jong Un's isolated dictatorship poses a deep threat to the US, up from 48% who said the same in March and the highest that figure has been in polling dating back to 2000.

That shift comes as 77% say they think North Korea is capable of launching a missile that would be able to hit the US.

## **Turkey is trying to get an ATOMIC BOMB in secret weapons plan, warns expert**

Source: <http://www.express.co.uk/news/world/838694/Turkey-atomic-bomb-Recep-Tayyip-Erdo-an-nuclear-weapon-fears>

Aug 07 – With tensions threatening to reach breaking point between the US and North Korea it has emerged Turkey could be trying to build up its weaponry [as relations with the EU reach a new low.](#) In a worrying claim, an expert has warned Turkey is the next country looking to expand its arsenal to include atomic bombs.

Abdullah Bozkurt, a government-critical Turkish journalist, has dramatically revealed what he called 'secret plans' for Ankara to acquire the ultimate weapon.

Despite Turkey having the second largest-NATO army, with President Recep Tayyip Erdogan presiding over 40,000 soldiers, Mr Bozkurt said his ambitions were far greater.

He stated there were plans for Ankara to expand, and a "secret plan to acquire weapons of mass destruction - including an atomic bomb for deterrence."

Influential advisors close to the President and a group of officials in the government's inner circle are said to have discussed acquiring an A-bomb, Mr Bozkurt said.

He outlined recent meetings with Russia and Japan, signalling a move away from NATO.

Mr Bozkurt said the talks focussed on the construction of two nuclear power plants in Turkey, arousing his suspicions.

And his fears seem to be bolstered by Turkish expert Aykan Erdemir, of the US Thinktank Foundation for Defense of Democracies.







Mr Erdemir, a former member of the Turkish parliament, said: "Erdogan has a strong desire to turn Turkey into a nuclear power, but doesn't have the capacity."

But he outlined obstacles to Mr Erdogan's perceived plans.

A little over a year on from a failed coup, which saw hundreds killed and heralded the dawn of a crackdown of public sector workers, Mr Erdemir said the Turkey's ability to get the project off the ground was compromised.

Despite teething problems, he identified popular demand for the country to be nuclear armed.

He said: "Turkey lacks financial resources and personnel for such an expensive and high-tech project.

"The government-friendly media often exaggerates the strength of the military to increase morale in Turkey."

**And continuing the purge of the armed forces beginning after the putsch, Mr Erdogan has fired 160 of the 324 generals of the Turkish army in the past few months.**

He has also culled thousands of soldiers from high ranking positions.

Mr Erdemir believes Mr Erdogan is rooting out any dissidents and anyone who would not back his nuclear dream.

The worrying claims coming out of Turkey come as Ankara finds itself embroiled in a political spat with the EU, particularly Berlin.

The bitter row has seen relations steadily deteriorate, with Mr Erdogan saying in April the EU "a continent that is rotting in every which way".

Recently Berlin issued new travel warnings for tourists visiting the country, and foreign minister Sigmar Gabriel said he could no longer guarantee investment in Turkey following accusations made by Mr Erdogan.

The President accused German companies of colluding with the man he views as his political enemy - and who he suspects was behind the failed coup last year - Fethullah Gülen.

And in a painful move for Ankara, Mr Gabriel added he would discuss with other EU leaders the prospect of reviewing pre-accession funds being offered.

## Would Charlotte Survive A Nuclear Bomb? There's An App For That.

Source: <https://patch.com/north-carolina/charlotte/would-charlotte-survive-nuclear-bomb-there-s-app>

Aug 08 – North Korea announced this week that its military might attack the U.S territory of Guam — prompting President Donald J. Trump to promise to meet any attack with "fire and fury like the world has never seen" — and there are concerns that a nuclear launch from the

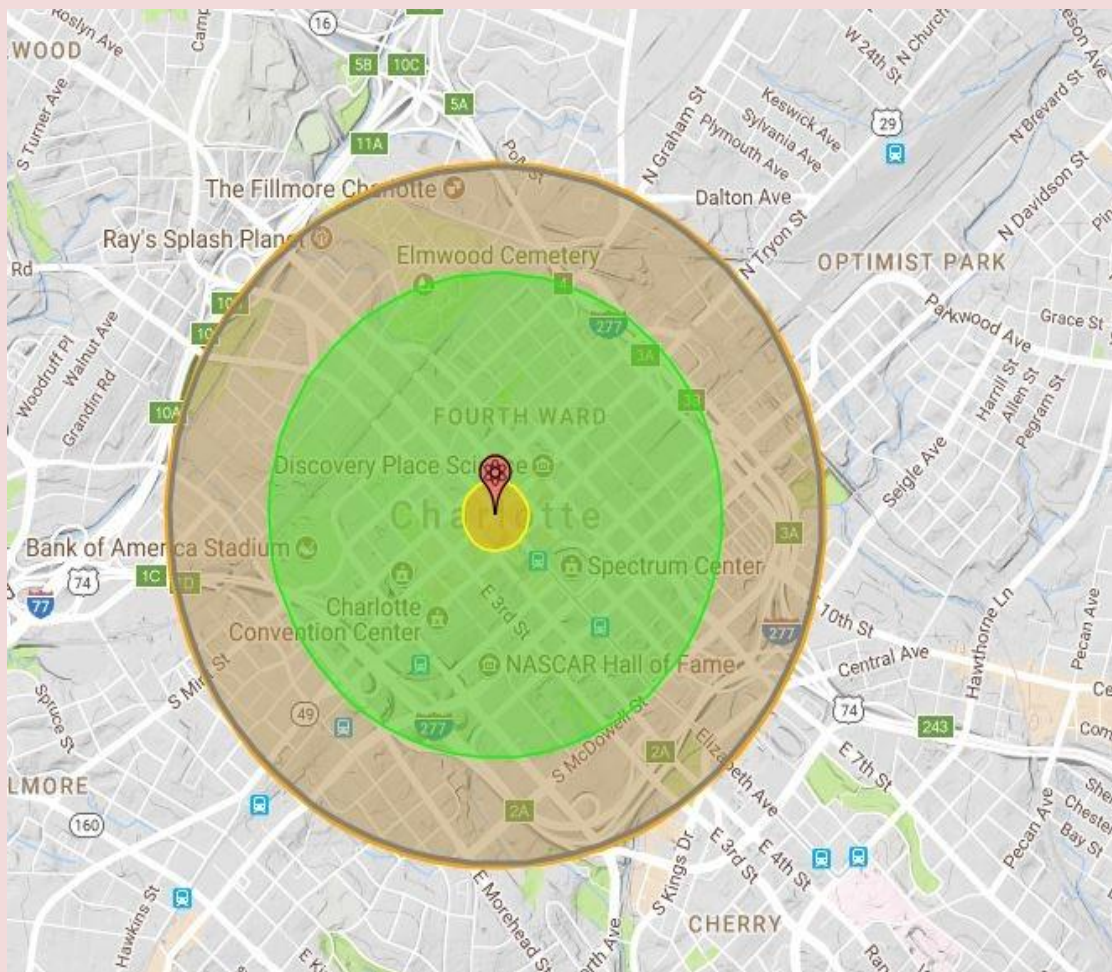


**CBRNE-TERRORISM NEWSLETTER – August 2017**

country could reach as far as Los Angeles, Chicago or even New York City. But what would really happen if a medium- or long-range missile with a nuclear bomb reached your city?

A web tool called NUKEMAP claims it can tell you. Straddling the line between entertainment, fantasy and terrifying reality, the Google Maps mashup is a tool for visualizing the real-world impact of a nuclear explosion on specific locations. Here's how it works:

Users choose their preferred weapon of mass destruction and their target by selecting from a list of pre-set cities or choosing a point on the map. Which bomb they choose depends on how much damage they want to do — are you aiming for total annihilation or do you just want to create a little chaos? Your choices start with the American-made "Davy Crockett," which is relatively benign when compared to the Russian-made "Tsar Bomba," a Russian-made bomb that means business.



NUKEMAP shows the potential impact on Charlotte of a nuclear weapon similar to that tested by North Korea in 2013/ NUKEMAP screenshot. Once the bomb is detonated, ringed circles appear around the targeted cities, showing the radius of the fireball, the radius of thermal radiation and an outer radius where buildings would likely survive the blast. It graphically displays the extent of injuries and damage to buildings from firestorms. (Get Patch real-time email alerts for the latest news in [Charlotte](#) — or [other neighborhoods](#). And iPhone users: Check out [Patch's new app](#).)

If a weapon similar to one North Korea tested in 2013 were detonated in Charlotte, for example, about 33,270 people would die and another 41,970 would be injured, according to [NUKEMAP](#). The rest of the scenario is pretty ugly, too, NUKEMAP says: "Without medical treatment, there can be expected between 50% and 90% mortality from acute (radiation) effects alone. Dying takes between several hours and several weeks."

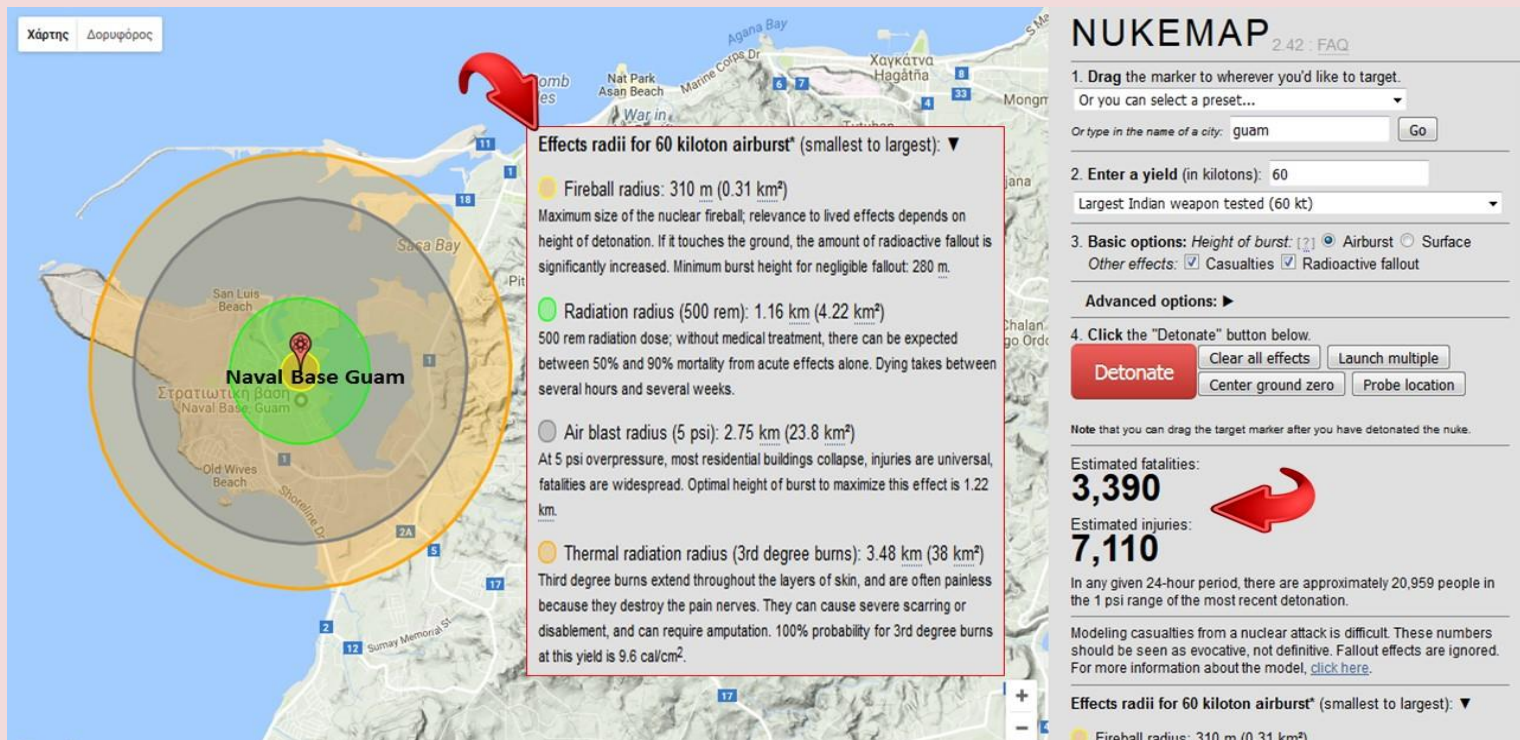
NUKEMAP was created five years ago by historian [Alex Wellerstein](#), who specializes the history of nuclear weapons and secrecy. Over the last five years, the website has hosted more than 99 million virtual detonations, Wellerstein wrote on his [nuclearsecrecy.com](#) blog.





## CBRNE-TERRORISM NEWSLETTER – August 2017

He said he typically sees viral spikes in site visits around the anniversaries of the bombings of Hiroshima on Aug. 6, 1945, and Nagasaki on Aug. 9, 1945.



An intercontinental ballistic missile launched Friday by North Korea burned out before reaching Japan, but its height and range indicated that [major U.S. cities like Chicago, L.A. and New York](#) could be within Kim Jong Un's scope, according to Newsweek.

## What the Crisis Means: North Korea, Nukes and Islamists

By Ryan Mauro

Source: <https://clarionproject.org/10-ways-north-korea-impacts-jihad-threat/>

Aug 09 – North Korea is officially a communist, Stalinist dictatorship, but that hasn't stopped it from crossing the ideological divide to embrace Islamist regimes and, reportedly, even jihadist groups. The latest crisis between North Korea and the U.S. appears separate from the war with [Islamism](#), but there are 10 ways it overlaps.

The U.S. and allied intelligence services now believe North Korea has [miniaturized its nuclear warheads](#) to fit onto its intercontinental ballistic missiles and has the potentially up to 60 nuclear weapons.

This was seen as an undeclared "red line" and prompted President Trump to threaten to bring "fire and fury like the world has never seen" if North Korea's verbal threats continue; a benchmark North Korea immediately crossed by announcing it was considering a nuclear strike on the U.S. territory of Guam, where 6,000 U.S. troops are stationed. Another 28,000 U.S. troops are in South Korea and 49,000 in Japan.

North Korea [threatened](#) to attack Guam in 2013 and its bombastic rhetoric is practically a daily occurrence, but North Korea's aggressive attacks have increased in recent years including sinking a South Korean ship in 2010, an artillery barrage on a South Korean island that same year, a cyber attack on Sony Pictures in 2014 and a bold assassination of a political rival in a Malaysian airport using the VX biological weapon earlier this year

**The Iranian and North Korean WMD programs should be seen as a single entity.**

We must now assume that Iran likewise has the ability to miniaturize nuclear warheads onto ICBMs.





**CBRNE-TERRORISM NEWSLETTER – August 2017**

Iran and North Korea have shared virtually everything when it comes to ballistic missile and nuclear technology. One Iranian opposition group [claimed](#) that Iran continued its nuclear program in spite of the nuclear deal by simply outsourcing it to North Korea. The nuclear and missile tests are widely seen as being on done [on behalf of Iran](#) with Iranian scientists on the scene for their occurrences.

Both North Korea and Iran helped the Syrian regime pursue nuclear weapons, resulting in the Israeli airstrike on Bashar Assad's nuclear reactor in 2007. Various reports indicate that Syria's nuclear program continued thereafter, albeit on a smaller scale.

**North Korea's Links to Hamas, Hezbollah and reportedly Al-Qaeda-tied terrorists in the Philippines.**

In 2003, the government of the Philippines [said](#) that it captured documents showing that the Moro Islamic Liberation Front, an Islamist group that has had a relationship with Al-Qaeda in the past, paid \$2 million to North Korea for guns, ammunition and grenades and was looking to buy mini-submarines. Another sale was [reported](#) in 2005 of 10,000 rifles.

In 2006, a federal judge [ruled](#) that North Korea is liable for damages caused to American-Israeli citizens due to its material support for Hezbollah. Iran sponsored North Korean assistance to help the terrorist group by providing rockets and missiles and guidance on building its sophisticated network of tunnels and bunkers. It said that Hezbollah terrorists have been traveling to North Korea for advanced training since the late 1980s.

In 2009, the UAE [intercepted](#) over 2,000 detonators for Hamas' 122mm Grad rockets and associated equipment. Later that year, Israel [intercepted](#) 35 tons of rockets, RPGs, shoulder-fired missiles and equipment for surface-to-air missiles from North Korea to Iran for delivery to the Hamas and Hezbollah terrorist groups in Thailand.

In 2014, it was [reported](#) that Hamas was negotiating an arms deal with North Korea worth hundreds of thousands of dollars for missiles and communications equipment and a down payment had already been made. It is strongly suspected that North Korea helped Hamas build its sophisticated tunnel system that was used to attack Israeli civilians and wage war in 2014 against the Israeli military.

The Hamas terrorist group [openly thanked](#) North Korea for its political support against Israel this year. The North Korean regime (DPRK) [pledged](#) to "mercilessly punish" Israel for its leaders' accurate description of the ruling leader as a "crazy." The DPRK said it "fully supports" the Palestinian [jihad](#) to have an independent country and to seize Jerusalem, a vague statement that seems to imply material support. We should expect such sales to increase as sanctions force the North Korean regime to look for more revenue, as well as ways to retaliate against the U.S. and its allies. The North Korean regime has no problem selling arms to Islamists and is not a target of the jihadists, so we shouldn't be surprised if North Korea goes so far as to directly sell weapons and expertise to groups like ISIS and Al-Qaeda.

**North Korea has threatened to sell nuclear weapons to other countries and even international terrorist groups. It now has up to 60 nuclear weapons, a number that could grow to [100 by 2020](#).**

In 2005, North Korea [threatened](#) to sell its nuclear weapons to terrorist groups "if driven into a corner."

North Korea has a surplus of nuclear weapons. It can afford to sell off a few if it feels confident that U.S. intelligence will be unable to identify and intercept the shipment; a fair assumption given our recent underestimations of their capabilities.

Past customers for Iranian missiles and arms include Iran and its puppet Assad regime in Syria; Yemen, which is now working with Salafists and the [Muslim Brotherhood](#); Pakistan; Eritrea, which has supported Al-Qaeda's branch in Somalia; the Somali government; Cuba and possibly Venezuela. There are [suspicions](#) that Turkey is looking to build nuclear weapons, as an [imam](#) close to President Erdogan is [encouraging this](#).

**Joint cyber warfare programs with Iran.**

Both Iran and North Korea have launched cyber attacks on the U.S. and its allies with minimal consequences. There is strong evidence that the two rogue states' programs are [interconnected](#) and they are even launching joint cyber attacks together.



**CBRNE-TERRORISM NEWSLETTER – August 2017****Radical Islam will seep into an unstable North Korea.**

As soon as a closed society begins opening up, the promoters of Islamism get to work. A relevant example is how Saudi Arabia, Qatar and Turkey are in a [mad dash](#) to lead the Muslim community in Cuba.

In 2010, Pew [estimated](#) there are 3,000 Muslims in North Korea, a 300% increase from 1990. It projects that number will stay about the same until at least 2030, but that is doubtful as globalization inevitably penetrates North Korea and exposes more citizens to Islam.

The most jihad-prone forms of Islam in North Korea are already leading the way. In 2013, North Korea [allowed Iran](#) to build the country's first mosque, located at the Iranian embassy.

The extreme anti-Americanism and anti-democracy thought that is instilled in the population means this Muslim population will probably be inclined towards radicalism.

**Regime instability will be a gold mine for terrorists, criminals and rogue states.**

The regime is bound to become more unstable over time and that could increase as international tension rises and the U.S. potentially tries to undermine Kim Jong-Un. North Korea is armed to the teeth with deadly expertise, conventional weapons and WMDs, all of which will be sold off by their hungry protectors or abandoned in the event of extreme upheaval.

All kinds of black market criminals, terrorists and governments will be trying to snatch up whatever they can. For Islamists, they will look to the Muslim population for logistical support. Iranian operatives are already in the country, as may be Hezbollah terrorists.

ISIS is on the rise in the Philippines, the Islamic terror threat is [increasing](#) in South Korea and it's only a matter of time before China's Muslim-majority Xinjiang Province becomes a jihadist front. North Korea is isolated now, but don't assume that Islamists won't be able to enter the country and make contact with its black market as the regime becomes unstable.

**Reported plans for a two-front war by Iran, Syria and North Korea.**

There have been intelligence reports since the early 1990s indicating that Iran, Syria and North Korea had a deal to force the U.S. into a two-front war if any one of them came into military conflict with America. Since then, these countries have only grown stronger, we have grown weaker, and their friendships have grown tighter.

Of course, we do not know if such an agreement exists today and we also do not know if they are loyal enough to honor it if it exists. However, the reported historical precedent must be taken into account and it is certain that Iran, Syria and North Korea will at least take limited measures to assist each other in the event of military conflict. And if Iran and North Korea have aspirations to commit aggression, there's no better time to act than when the U.S. is preoccupied on another front.

**Bogging down the U.S.**

If the situation escalates, then the U.S. military—already suffering from the [sequestration](#)—will be hard pressed for resources to maintain its operations against ISIS, Al-Qaeda and the Taliban in Iraq, Syria and Afghanistan, not to mention more limited efforts in places like Yemen, Libya and the Philippines.

**North Korean Terrorists Could Target U.S. Soil**

It is not out of the realm of possibility that North Korea will try to launch saboteur/terrorist attacks on American soil, particularly against those seeking to undermine Kim Jong-Un.

Earlier this year, Kim Jong-Un used two assassins to murder a political rival using the VX biological weapon in a Malaysian airport. Think about how much of an escalation that is: A biological terrorist attack inside an airport in a foreign country. That means North Korea has loyal operatives who can sneak such deadly substances into other countries and are willing to risk their lives to commit murder on Kim Jong-Un's behalf.

And the target was another North Korean from the top of society. Such operatives would have even less qualms about targeting Americans.

North Korea could collaborate with Islamist terrorists or criminal elements for an attack in America. After all, the Iranian Revolutionary Guards Corps hoped to hide behind Mexican drug cartel members in its plan to kill the Saudi ambassador in Washington D.C. by blowing up a diner.



**CBRNE-TERRORISM NEWSLETTER – August 2017****The Worst of All Scenarios: EMP**

Watch [this Clarion Project short film from 2012](#) about the threat posed by a potential Electro-Magnetic Pulse attack by Iran. North Korea has the same capability. A top expert on nuclear weapons and EMPs, Dr. Peter Vincent Pry, has been [sounding the alarm](#) that he believes North Korea is actually practicing carrying out such an attack on the U.S.

Should that happen and the attack succeed, North Korea will cripple the U.S. and perhaps win its war against America. And even if the U.S. destroyed North Korea in response, the jihadists will have won *their* war against America as the country struggles to survive as Islamists rampage across the planet.

*Ryan Mauro is ClarionProject.org's Shillman Fellow and national security analyst and an adjunct professor of counter-terrorism.*

## **Pyongyang can miniaturize, so let's move on to what's important: David Wright on the North Korea crisis**

By Lucien Crowder

Source: <http://thebulletin.org/pyongyang-can-miniaturize-so-let%E2%80%99s-move-what%E2%80%99s-important-david-wright-north-korea-crisis11003>



Aug 10 – On Tuesday, *The Washington Post* set the arms control community abuzz with its [reporting](#) on a US intelligence assessment that North Korea had gained the capability to make nuclear warheads small and light enough to be mounted on Pyongyang's newly operational intercontinental ballistic missiles. Later the same day, President Trump set a much larger cross-section of the world abuzz with his declaration that North Korea would “be met with fire and fury like the world has never seen” if it continued to issue threats toward the United States. Soon the nuclear stand-off on the Korean Peninsula, often described as a Cuban Missile Crisis in slow motion, began to feel like a Cuban Missile Crisis in real time. But according to David Wright—an expert on nuclear and missile issues with the Union of Concerned Scientists—the *Post* story contains few real surprises and Trump's “fire and fury” rhetoric is unlikely to alter the basic calculus of self-preservation that stands paramount in Pyongyang. Still, Wright argues, a “crisis mentality” and an error of some kind could add up to disaster on the peninsula.

**Bulletin:** First, I wonder if you could clarify one point just for my understanding. My reading of Tuesday's *Washington Post* story is that this new intelligence assessment about miniaturization is delivered by the Defense Intelligence Agency (DIA), but it represents a

summary assessment of the entire intelligence community. Have I got that right?

**David Wright:** I have wondered that myself. People I've talked to point out that the DIA has released several presumably classified assessments about North Korea





## CBRNE-TERRORISM NEWSLETTER – August 2017

recently and wonder what's going on, and whether these are consensus views or DIA views. Statements by officials in other parts of the intelligence community suggest there are other views, so I'm not sure what to think at this point.

**Bulletin:** I understand that you don't have access to all the same information that the intelligence community has, but do you know of concrete information that justifies a change in assessment regarding miniaturization?

**DW:** No. I don't know what that's based on.

**Bulletin:** So there's nothing new here that we can see.

**DW:** I think that's right—though it doesn't particularly surprise me. But I don't know why they've come out with this now.

**Bulletin:** I wonder if you could quickly explain what's hard about miniaturization in the first place.

**DW:** If you're trying to develop a nuclear weapon, and you want a device that will go off, you tend to not worry about minimizing everything as much as you could. You tend to use more fissile material than you think you probably need. You tend to use more high explosives so you get a good compression. Once you have that working, then you have to figure out "How can I shave off some of the mass and still have a reliable warhead? How do I make sure that I've gotten the masses down to the point that I'm comfortable with and still believe that I have enough reliability and confidence that this thing will go off when I want it to?"

**Bulletin:** Are there different stages of miniaturization capability? For instance, is it one thing to miniaturize enough for a short-range missile, but a different thing to miniaturize for a medium-range missile or an intercontinental ballistic missile (ICBM)?

**DW:** Well, in practice it is, because if you look at developing ballistic missiles, it turns out that it's relatively easy to make short-range missiles. So, for example, with the Scud missile that the Soviets were building, the body was made of steel, it carried a tonne warhead, and yet they could still put an engine in it that would get it up to high enough speed that it could go for 300 kilometers. Now, the problem is that once you try to increase the range, it gets harder and harder. So what you want to start doing is shaving mass off wherever you can, and so you start making the body out of lighter-weight materials. That gets you a certain distance. But

at some point you decide you want to start staging because, if you use multiple stages, you burn part of the fuel and then drop the casing for that, and you've got less mass to accelerate. As you go longer and longer in range, you're trying to do more and more to shave off mass. Launching one tonne on a short-range missile would be relatively easy. Launching that same mass on a long-range missile is quite a bit more difficult. For that purpose, you'd like to have a lighter-weight warhead to carry.

And the same is true with the re-entry vehicle. You also want to have the heat shield that can get the thing down through the atmosphere at these high speeds, and that also gets harder and harder for long range because it re-enters at higher and higher speeds. That means you've got more and more heating. And again, you'd like to convince yourself that you've shaved off as much mass as you can, but that you still have enough left to protect the warhead and not to mechanically fail during re-entry. So all those things add up to pretty serious engineering problems.

**Bulletin:** I've got a couple of questions about re-entry, actually. What's your assessment of the timeline reported in the *Post* story that the North will be able to field a workable re-entry vehicle by late next year?

**DW:** I think that that's probably right, assuming they haven't already done it. There are trade-offs with re-entry vehicles. The easiest way to get a warhead down to the ground and not have it overheat is to have a very blunt warhead and have it slow down high in the atmosphere, so that by the time it gets to the lower part of the atmosphere—where the atmospheric density is higher—it's moving much slower and the heating is less intense. And if you think about it, the early Mercury and Gemini capsules came in basically backwards, and they had that very broad back end. It was their way of dealing with the heating, it slowed them down very high in the atmosphere and they came down much more slowly. I think there's no doubt that North Korea could put a fairly blunt re-entry vehicle on its warheads and get them to the ground without a problem on the heating.

The problem is that, when you slow down the re-entry through the atmosphere, you get much higher inaccuracy. Now, that may or may not be a problem [from North Korea's perspective]. There are sort of two large parts to the inaccuracy of a blunt missile. One



## CBRNE-TERRORISM NEWSLETTER – August 2017

is that you aim a missile by controlling its speed and the angle it's going when the engines burn out a couple of minutes after it's launched. Now, if you don't have very good control over both the angle and the speed, or if you don't have a very good accelerometer in the missile—so it doesn't know exactly how fast it's going—then all those things will add up, especially for a long-range missile, to a big miss distance. And similarly, atmospheric winds, density variations, whether it's wobbling or tumbling—all those things put lateral forces on it, and so again, you can get a big contribution to errors due to re-entry. And so if North Korea was launching a long-range missile at a target, I think they'd be lucky to get within tens of miles of that point.

So you can ask yourself, well, "How worried should they be about losing a little bit more accuracy by having a blunt warhead on re-entry?" I don't know how they're thinking about that trade-off. But certainly they could deal with re-entry by having a blunter body. Now in the last launch, on July 28th, there is some video footage from a camera in Japan that seems to show a glowing body coming down during re-entry, and then it stops glowing at some point. And the interpretation that some people have is that it got to the point that it mechanically failed and broke up a couple of kilometers above the ground. I don't know if that's right. It's not a crazy interpretation of what we're seeing, but I'm not sure it's the right interpretation. If it's true, it may mean that North Korea is sort of pushing the envelope on this, and is trying to increase its accuracy by having a relatively streamlined re-entry vehicle, and that has caused them to run into some problems. But I don't see that as a fundamental problem. I think they could design, as I was saying before, a more blunt re-entry vehicle that would allow the warhead to get to the ground.

**Bulletin:** If they're satisfied with hitting a target the size of Los Angeles... somewhere...

**DW:** Yeah, which is I think the best they can do anyway, for the foreseeable future. Getting long-range missile accuracy down below kilometers is really difficult. If you look at the extent of the work that the US and Soviet Union did on really getting the details of guidance and control down, on mapping the gravitational field of the Earth so they could do the calculations to figure out more accurately how they should aim it—and then they worked very, very hard on coming up with new materials and ablative coatings on their warheads and figuring out how to make that

coating work in a symmetric way. It took a tremendous amount of work. So I think for the foreseeable future, North Korea is talking about city-sized inaccuracy for its warheads.

**Bulletin:** I see. So the biggest technical problem facing them at this point isn't exactly miniaturization and it isn't a workable re-entry vehicle. It's good targeting.

**DW:** Yeah... Although, again, if what you're trying to do is hit Los Angeles, that's a pretty damn big target.

**Bulletin:** Returning to ICBMs themselves, it sounds as if there's a consensus that North Korea has been testing what you could call ICBMs, but that view isn't entirely universal. So in your opinion, putting aside re-entry and miniaturization, is the belief that North Korean missiles can now reach the continental US well-founded?

**DW:** Oh, absolutely. So... let me put a caveat on that. Take the most recent launch, July 28th. The information I had was a range of about 1,000 kilometers; the flight time, when they shot it up on a highly lofted trajectory till it came down, which was about 46, 47 minutes; and the maximum altitude that it went up to, which was, I think, about 3,700 kilometers. So what I did was to model these things in my computer and I said "Let me look at a missile that would have enough speed to go up to 3,700 kilometers and then come down at a range of 1,000 kilometers. How long does that fly?" And it turns out it's about 46, 47 minutes. So those numbers were all consistent with each other. And we've seen from what North Korea has released that that's sort of what they were trying to do. So I think there's agreement that that's basically what they did.

And then you can ask the question, well, if you have a missile that gives you enough speed to fly that trajectory, and instead of shooting it almost straight up, you shot it on a more standard trajectory for an ICBM, how far would it go? That gives you well, well over ICBM range. I think the major hold-out on this [issue] has been the Russians. The Russians seem to have political reasons for not wanting to admit that North Korea has long-range missiles. They have been giving some very odd information about what they've seen, which seems to sort of correspond just to the first stage of this missile. I don't think anybody really understands why the Russians seem to be saying that North Korea doesn't have ICBM



## CBRNE-TERRORISM NEWSLETTER – August 2017

capability. As far as I can tell, everybody else [believes North Korea has ICBM capability]. If the information that came out about the lofted trajectory on July 28th is right, that same missile would definitely have ICBM capability along a standard trajectory.

**Bulletin:** Returning to an earlier theme—correct me if I'm wrong, but it seems to me that the intel community consistently estimates North Korea's capabilities higher than many nongovernmental experts might, or at least they reach conclusions about new capabilities more quickly than outside experts do. That seems to apply to miniaturization, to arsenal size, and so forth. Why do you think these estimates come out on the high side? Does the intelligence community just know more than everyone else? Do they assess better than everyone else? Or is my impression wrong to begin with?

**DW:** What we saw for a long time was the intelligence community coming out with estimates of—I'm going back 15 years or so—they were coming up with estimates for when they thought North Korea might have a long-range missile. And those tended to be on the short side. They tended to see this capability coming faster than most outside experts did. We don't know the details of the analysis, but it could have been a worst case—if you're trying to plan for this stuff and you don't want to be taken by surprise. So that was a case where most outside experts, having watched the program, thought that the intelligence coming out was too aggressive. My sense is, more recently, that hasn't necessarily been true. There are certainly outside experts who have been saying for quite some time that they thought North Korea had the ability to miniaturize. Jeffrey Lewis [director of the East Asia Nonproliferation Program at the Middlebury Institute of International Studies] is a good example of that. There are certainly others. I've come around to that view for some time now. Some people have said that it looks like when it was convenient to overestimate the threat—for example, to buttress the funding for missile defense—they did that. Now, when it's starting to look like a more serious threat and they don't know what to do about it, they're sort of hedging their bets a little bit. I'm not sure there's a clean answer to that, to be honest—who's overestimating and who's underestimating. Because I know there have been, certainly, frustrations. Jeffrey Lewis is one of the key people—he's been very frustrated with a lot of assessments of North Korea that

seem to downplay their ability to do some of the things that they appear to have done.

**Bulletin:** I see. Well, in any case it sounds more complicated than I thought it was. In your own calculations and assessments about North Korea, what are the greatest areas of uncertainty for you? Where do you have the most trouble deciding what you believe?

**DW:** Well, [regarding] missiles with very long ranges, one of the things we don't understand is what payload those were launched with. For example, if you look at the July 4th launch, which we estimated to have a range of something like 7,000 kilometers if it was fired as an ICBM, and then you look at the July 28th launch, which had a much longer range than that—longer than 10,000 kilometers—in my modeling I could cause that difference by assuming that the July 4th test had essentially a full warhead in it, maybe half a tonne, and the July 28th test had a much smaller payload. [That is], they might not have put in the full mass of a mock warhead—they might have sort of flown the re-entry vehicle empty. So one possibility is that they wanted to really make the point that they could hit the US, and they off-loaded payload to get that longer range. On the other hand, there are things we see they could have done, in terms of some modifications to the second stage of the missile, that may have allowed them to reach these longer ranges with sort of a full-size payload that would be comparable to a nuclear warhead. That's one of the really interesting questions that we're trying to look at in the modeling. If we make reasonable assumptions about what this missile looks like, can we start to get a feel for whether or not this long range was achieved with a large payload or not?

**Bulletin:** On to my next-to-last question. Please share your thoughts on the fire and the fury.

**DW:** I think, and a lot of people agree with this, that Kim Jong-un may be a despicable human being, but he's not irrational. I think he recognizes that, if he launched an attack, it would lead to a response that would destroy his regime, and one of the things that he really cares about is staying in power and keeping the regime alive. So I don't expect him to wake up one day and just decide to launch at Los Angeles or Tokyo. What I am concerned about is that, as tensions increase between North Korea and the United States, and they get in a crisis mentality, something could happen—by mistake, by





**CBRNE-TERRORISM NEWSLETTER – August 2017**

misinterpreted signal, things like that. And in particular, if you read some of the official statements that have come out of North Korea in the last couple of days, they go through a list of things that they say they see the US doing, like reinforcing bombers on Guam, and using those bombers to do overflights of the Korean Peninsula. They say the United States has conducted more ICBM flight tests out over the Pacific than they have in the past. So North Korea is starting to see activity that they can interpret as threatening. There's about to be another set of exercises involving the United States and South Korea, which North Korea sees as practice for an invasion of the North. It seems to me when you add these bellicose statements [in which] the United States is threatening to use what, from the wording, certainly sounded like nuclear weapons, it makes me even more worried about a really devastating crisis because of miscalculation, misperception. Using language like that and continuing to up the ante—I worry about that quite a bit. What I really think the US needs to do is just the opposite, try and calm things down and make sure they don't get out of control. Then, through diplomatic effort, try to open a line of communication with North Korea that, for example, would put a freeze on testing nuclear weapons and missiles, and try to set the stage for a longer-term negotiation that would deal with some of the more fundamental issues.

**Bulletin:** What chances do you give the scenario you just described?

**DW:** You know, I wish I knew the answer to that. We're hearing from military advisors like Secretary of Defense Mattis that there's no good military option. We're hearing from [Secretary of State] that we are not enemies of North Korea, we are not trying to do regime change. You're hearing the right words from those people—that they recognize that diplomacy is the best of all the bad options on the table. On the other hand, you're hearing things like the stuff that was coming from President Trump [on Tuesday], which seems to undercut all that. Having watched President Trump for six months now, it's clear that he likes to—and I think he sees this as part of his bargaining—come out with really strong positions and then walk back from there. And maybe that's what he's doing. In the past, he has said he'd be willing to sit down, talk, have a hamburger with Kim Jong-un. The problem is,

I don't think anyone knows where the center of that discussion in the administration is.

One of the things that the Trump administration has put a lot of hope on is China solving this problem. I think people should recognize that that's not going to happen, for a couple of reasons. One is that China sees the situation very differently. First, they don't feel like they have as much leverage as the United States thinks they do—without causing real instability in the region. And they also see this as fundamentally an issue between North Korea and the United States, and feel it has to be resolved by those two countries. So I think they're willing to facilitate negotiations, but they're not going to solve the problem. They also look at North Korea at this point and, according to people we've talked to over there, see themselves back in the 1960s and 1970s, when they were developing a nuclear program and were being sanctioned by the outside world. It basically strengthened their resolve to move forward with these programs. For that reason they believe that isolating North Korea and trying to starve it out is not going to work, and it's going to be destabilizing. That's one of the reasons they've continued to trade with North Korea. I think they feel that, in the same way that they were able to come out of that [experience] and become a more normal country, economic stability and some development of North Korea might help. Now, they may be wrong, but I think this idea that they're somehow going to strangle North Korea for the United States is not going to help.

If the administration realizes that sanctions can put pressure on but are not going to solve the problem, and that there are no good military options, then it seems to me they are sort of wedded to the possibility of negotiating. But I would have made the same argument under the Obama administration. They did try some negotiations, got burned, and then sort of stepped back and let North Korea go forward with its development program. One possible outcome is that the two countries remain at loggerheads and North Korea becomes not an accepted but a de facto nuclear state. Things go along in parallel and relations between the two countries don't really improve. That, again, would not be a good situation—because of the dangers of crises blowing up and things getting out of control.



*Lucien Crowder oversees the Bulletin's coverage of chemical weapons, biological weapons, and emerging technologies such as artificial intelligence, autonomous weapons, and cyber issues. He joined the Bulletin in 2012 to launch its Development and Disarmament Roundtable series, a feature that ran through the end of 2016. From 2006 through 2011, Crowder was associate editor at Current History, a monthly magazine devoted to contemporary international affairs. He began his journalism career in Taiwan, where he reported for a business magazine, edited for a daily newspaper, and published freelance articles on topics ranging from economics to the arts.*

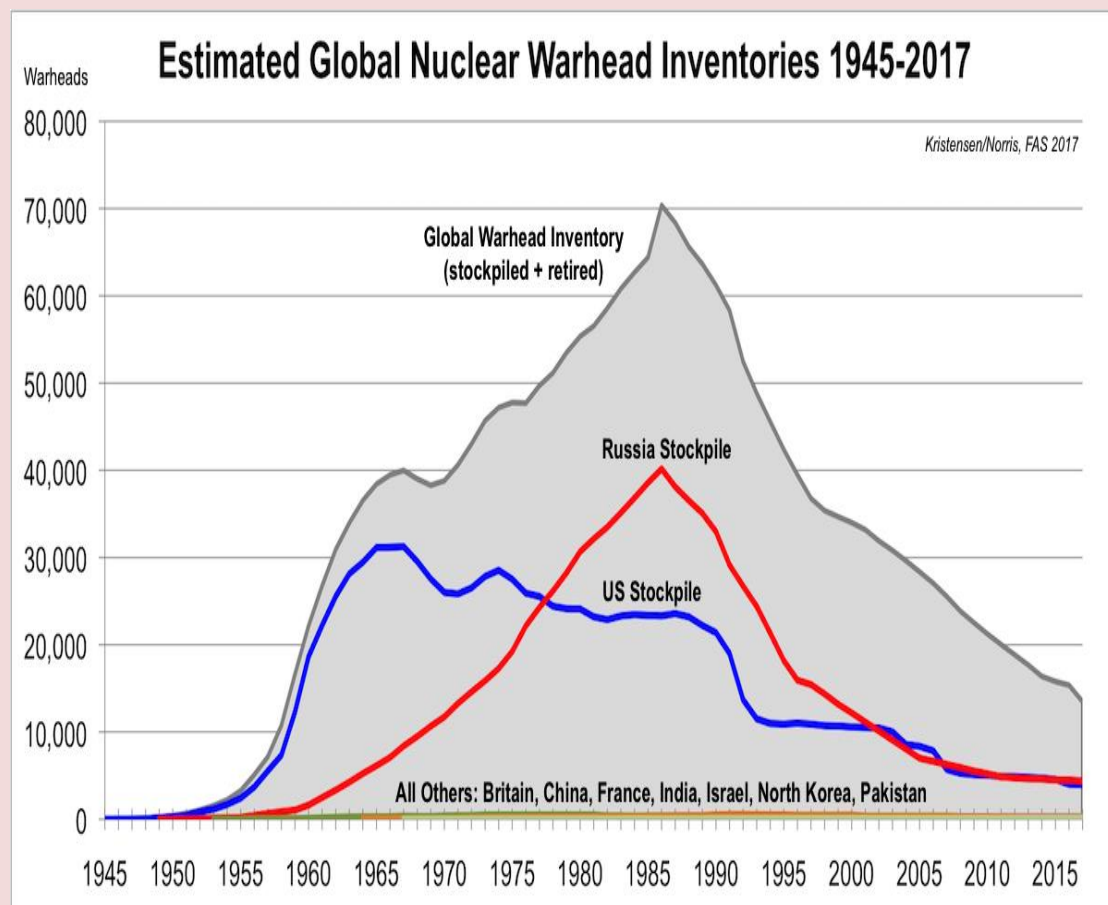
## Status of World Nuclear Forces

By Hans M. Kristensen and Robert S. Norris

Source: <https://fas.org/issues/nuclear-weapons/status-world-nuclear-forces/>

The number of nuclear weapons in the world has declined significantly since the Cold War: down from a peak of approximately 70,300 in 1986 to an estimated 14,900 in early-2017. Government officials often portray that accomplishment as a result of current arms control agreements, but the overwhelming portion of the reduction happened in the 1990s. Moreover, comparing today's inventory with that of the 1950s is like comparing apples and oranges; today's forces are vastly more capable. The pace of reduction has slowed significantly. Instead of planning for nuclear disarmament, the nuclear-armed states appear to plan to retain large arsenals for the indefinite future.

Despite progress in reducing Cold War nuclear arsenals, the world's combined inventory of nuclear warheads remains at a very high level: approximately 14,930 warheads as of mid-2017. Of these, roughly 9,400 are in the military stockpiles (the rest are awaiting dismantlement), of which more than 3,900

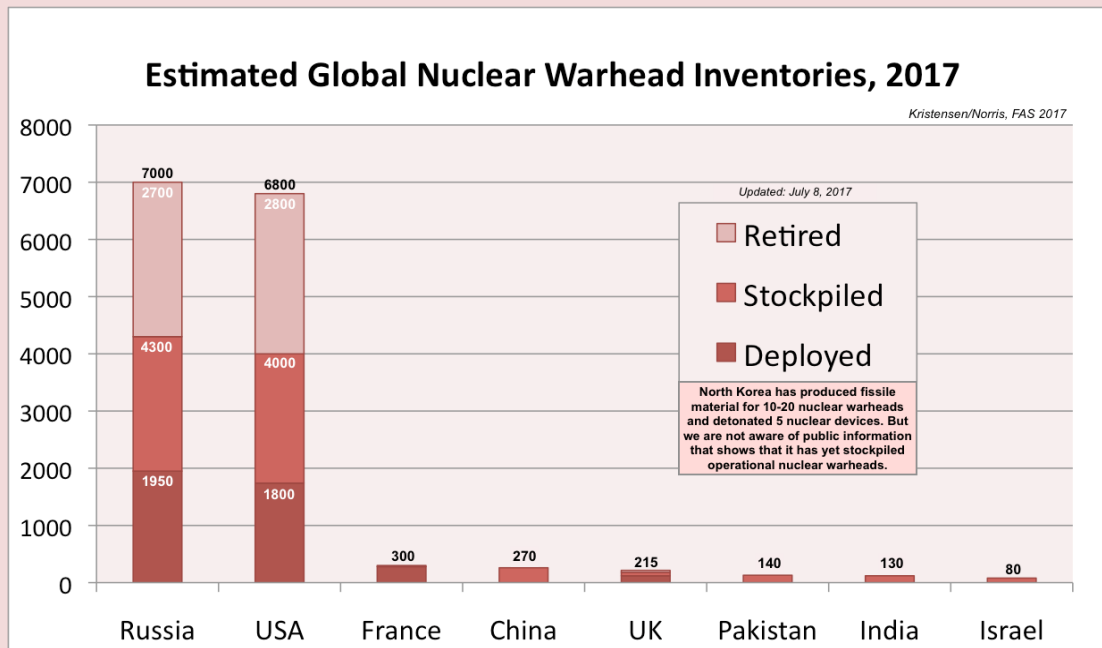


warheads are deployed with operational forces, of which nearly 1,800 US, Russian, British and French warheads are on [high alert](#), ready for use on short notice.



**CBRNE-TERRORISM NEWSLETTER – August 2017**

Approximately 93 percent of all nuclear warheads are owned by Russia and the United States who each have roughly 4,000-4,500 warheads in their military stockpiles; no other nuclear-armed state sees a



need for more than a few hundred nuclear weapons for national security:

The United States, Russia and the United Kingdom are reducing their warhead inventories, but the pace of reduction is slowing compared with the past 25 years. France and Israel have relatively stable inventories, while China, Pakistan, India and North Korea are increasing their warhead inventories.

All the nuclear weapon states continue to modernize their remaining nuclear forces and appear committed to retaining nuclear weapons for the indefinite future. For an overview of global modernization programs, see [this 2014 article](#).

The exact number of nuclear weapons in each country's possession is a closely held national secret. Despite this limitation, however, publicly available information, careful analysis of historical records, and occasional leaks make it possible to make best estimates about the size and composition of the national nuclear weapon stockpiles:

**Status of World Nuclear Forces 2017\***

Country	Deployed Strategic	Deployed Nonstrategic	Reserve/Nondeployed	Military Stockpile <sup>a</sup>	Total Inventory <sup>b</sup>
Russia	1,950 <sup>c</sup>	0 <sup>d</sup>	2,350 <sup>e</sup>	4,300	7,000 <sup>f</sup>
United States	1,650 <sup>g</sup>	150 <sup>h</sup>	2,200 <sup>i</sup>	4,000 <sup>j</sup>	6,800 <sup>k</sup>
France	280 <sup>l</sup>	n.a.	10 <sup>l</sup>	300	300
China	0 <sup>m</sup>	?	270	270	270 <sup>m</sup>
United Kingdom	120 <sup>n</sup>	n.a.	95	215	215 <sup>n</sup>
Israel	0	n.a.	80	80	80 <sup>o</sup>
Pakistan	0	n.a.	120-130	120-130	120-130 <sup>p</sup>
India	0	n.a.	110-120	110-120	110-120 <sup>q</sup>
North Korea	0	n.a.	?	?	? <sup>r</sup>
<b>Total:<sup>s</sup></b>	<b>~4,150</b>	<b>~150</b>	<b>~5,300</b>	<b>~9,400</b>	<b>~14,930</b>

**How to read this table:** Deployed strategic warheads are those deployed on intercontinental missiles and at heavy bomber bases. Deployed nonstrategic warheads are those deployed on bases with operational short-range delivery systems. Reserve/Nondeployed warheads are those not deployed on launchers and in storage (weapons at bomber bases are considered deployed). The military stockpile includes warheads that are in the custody of the military and earmarked for use by commissioned deliver vehicles. The total





**CBRNE-TERRORISM NEWSLETTER – August 2017**

inventory includes warheads in the military stockpile as well as retired, but still intact, warheads in queue for dismantlement. For additional guidance, see endnotes below.

\* All numbers are approximate estimates and further described in our [FAS Nuclear Notebooks](#) published in the *Bulletin of the Atomic Scientists*, and the World Nuclear Forces overview in the [SIPRI Yearbook](#). See also [status and 10-year projection](#) of U.S. and Russian forces. Additional reports are published on the [FAS Strategic Security Blog](#). Unlike those publications, this table is updated continuously as new information becomes available. **Current update: July 8, 2017.**

<sup>a</sup> Warheads in the “military stockpile” are defined as warheads in the custody of the military and earmarked for use by military forces.

<sup>b</sup> The “total inventory” counts warheads in the military stockpile as well as retired, but still intact, warheads awaiting dismantlement.

<sup>c</sup> This number is higher than the aggregate data under the [New START treaty](#) because this table also counts bomber weapons at bomber bases as deployed. [Detailed overview of Russian forces as of 2017 is here](#). Numbers have been updated for later changes.

<sup>d</sup> All are declared to be in central storage. Several thousand retired non-strategic warheads are awaiting dismantlement

<sup>e</sup> Includes an estimated 500 strategic warheads and all 1,850 non-strategic warheads.

<sup>f</sup> In addition to the 4,300 in the military stockpile, an estimated 2,700 retired warheads are estimated to be awaiting dismantlement. Details are scarce, but we estimate that Russia is dismantling 300-500 retired warheads per year. [See 2017 overview of Russian forces here](#).

<sup>g</sup> This number is higher than the aggregate data released under the [New START data](#) because this table also counts bomber weapons on bomber bases as deployed. [Detailed overview of U.S. forces as of 2017 is here](#). The US numbers have been updated to account for recent developments.

<sup>h</sup> Approximately 150 B61 bombs are deployed in Europe at six bases in five countries (Belgium, Germany, Italy, Netherlands and Turkey). For details, [see here](#) and [here](#) [update coming soon].

<sup>i</sup> Non-deployed reserve includes an estimated 2,050 strategic and 150 non-strategic warheads in central storage.

<sup>j</sup> The U.S. government [declared](#) in January 2017 that its stockpile included 4,018 warheads as of September 2016. Since then, a small number of warheads are thought to have been retired for an estimated 4,000 remaining in the stockpile.

<sup>k</sup> In addition to the roughly 4,000 warheads in the military stockpile, the US government in January 2017 announced that approximately 2,800 retired warheads are awaiting dismantlement. In addition, more than 20,000 plutonium cores (pits) and some 5,000 Canned Assemblies (secondaries) from dismantled warheads are in storage at the Pantex Plant in Texas and Y-12 plant in Tennessee. For detailed overview of U.S. forces, [see here](#).

<sup>l</sup> Only weapons for France's single aircraft carrier are not considered deployed, although it is possible that warhead loadings on some submarines missiles have been reduced. For a detailed overview of French nuclear forces, see [this 2015 article](#).

<sup>m</sup> China is thought to have “[several hundred warheads](#),” far less than the 1,600-3,000 that have been suggested by some. None of the warheads are thought to be fully deployed but kept in storage under central control. The existence of a Chinese non-strategic nuclear arsenal is uncertain. The Chinese arsenal is increasing with production of new warheads for DF-31/31A and JL-2 missiles. [Detailed overview of Chinese forces as of 2016 is here](#). Next China update: Summer 2017.

<sup>n</sup> The number of British warheads on each submarine has been lowered from 48 to 40. This has lowered the number of “operationally available” warheads from 160 to 120. By the mid-2020s, the stockpile will be reduced to “not more than 180.” This reduction is already underway. [Detailed overview of British forces is here](#).

<sup>o</sup> Although Israel has produced enough plutonium for 100-200 warheads, the number of delivery platforms and estimates made by the U.S. intelligence community suggest that the stockpile might include approximately 80 warheads. [Detailed 2014 overview of Israeli forces is here](#).

<sup>p</sup> None of Pakistan's warheads are thought to be deployed but kept in central storage, most in the southern parts of the country. More warheads are in production. [Detailed overview here](#).

<sup>q</sup> Indian nuclear warheads are not deployed but in central storage. More warheads are in production. [Detailed overview of Indian forces is here](#).

<sup>r</sup> Despite five North Korean nuclear tests and an estimate inventory of fissile material to potentially produce 10-20 nuclear warheads, there is no publicly available evidence that North Korea has operationalized nuclear warheads for delivery on ballistic missiles.

<sup>s</sup> Numbers may not add up due to rounding and uncertainty about the operational status of the four lesser nuclear weapons states and the uncertainty about the size of the total inventories of three of the five initial nuclear powers.

The information available for each country varies greatly, ranging from the most transparent nuclear weapons state (United States) to the most opaque (Israel). Accordingly, while the estimate for the United States is based on “real” numbers, the estimates for several of the other nuclear weapon states are highly uncertain.

*Hans M. Kristensen is director of the Nuclear Information Project at the Federation of American Scientists where he provides the public with analysis and background information about the status of nuclear forces and the role of nuclear weapons. He specializes in using the Freedom of Information Act (FOIA) in his research and is a frequent consultant to and is widely referenced in the news media on the role and status of nuclear weapons. His collaboration with researchers at NRDC in 2010 resulted in an estimate of the size of the U.S. nuclear weapons stockpile that [was only 13 weapons off the actual number declassified by the U.S.](#)*



**CBRNE-TERRORISM NEWSLETTER – August 2017**

government. Kristensen is co-author of the Nuclear Notebook column in the Bulletin of the Atomic Scientists and the World Nuclear Forces overview in the SIPRI Yearbook. The Nuclear Notebook is, according to the publisher, “widely regarded as the most accurate source of information on nuclear weapons and weapons facilities available to the public.”

**Dr. Robert Standish Norris** joined FAS in July 2011 as a senior fellow for nuclear policy. Dr. Norris was a senior research associate with the Natural Resources Defense Council in Washington, DC from 1984 to his retirement in 2011. His principal areas of expertise include writing and research on all aspects of the nuclear weapons programs of the United States, Soviet Union/Russia, Britain, France, and China, as well as India, Pakistan, and Israel. He was co-editor of NRDC's Nuclear Weapons Databook series and was a co-author of U.S. Nuclear Warhead Production, Volume II (1987); U.S. Nuclear Warhead Facility Profiles, Volume III (1987); Soviet Nuclear Weapons, Volume IV (1989); and British, French and Chinese Nuclear Weapons, Volume V (1994). More recent books include Making the Russian Bomb: From Stalin to Yeltsin (1995) and Atomic Audit: The Costs and Consequences of U.S. Nuclear Weapons Since 1940 (1998), with other authors. He has co-authored or contributed to the chapter on nuclear weapons in the 1985 – 2000 editions of the SIPRI Yearbook. He has written articles for Arms Control Today and Security Dialogue, and has authored a column for the Bulletin of the Atomic Scientists since 1987. He co-authored the online/DVD article on “Nuclear Weapons” of the Encyclopedia Britannica. He wrote a biography of General Leslie R. Groves, the head of the Manhattan Project that built the atomic bomb during World War II. The book, Racing for the Bomb: General Leslie R. Groves, the Manhattan Project's Indispensable Man (Steerforth Press, 2002) has been favorably reviewed in the New York Times, WashingtonPost, Foreign Affairs, Bulletin of the Atomic Scientists, Assembly, U.S. Naval Institute Proceedings, and The Journal of Military History among other publications and won the Distinguished Writing Award for best Biography of 2002 from the Army Historical Foundation. Dr. Norris received his Ph.D. in Political Science from New York University in 1976, and has taught at New York University, Miami University in Oxford, Ohio, Miami University's European campus in Luxembourg, and American University in Washington, DC.



## **NK has 13-30 nuclear weapons, and will have up to 60 nukes by 2020**

Source: <http://www.homelandsecuritynewswire.com/dr20170810-nk-has-1330-nuclear-weapons-and-will-have-up-to-60-nukes-by-2020>

Aug 10 – David Albright of the Institute for Science and International Security, prepared a useful [PowerPoint presentation](#) on North Korea's nuclear capabilities. He says that the best way to [summarize](#) the presentation, which offers the best available estimates of plutonium, weapon-grade uranium (WGU), and nuclear weapons in the possession of North Korea, is to use ranges of the medians of each case considered.

### **As of the end of 2016**

- ▶ 33 kilograms of separated plutonium (median value of a distribution).
- ▶ 175-645 kilograms of weapon-grade uranium, where 175 kilograms corresponds to a median estimate for the case of one centrifuge plant and 645 kilograms corresponds to the median estimate for the case of two centrifuge plants.
- ▶ 13 to 30 nuclear weapons, where these values reflect the utilization of 70 percent of the available, estimated stocks of plutonium and weapon-grade uranium. The limits correspond to the median values for the cases of one or two centrifuge plants and each weapon contains either plutonium or weapon-grade uranium.
- ▶ Based on this cumulative estimate, North Korea is currently expanding its nuclear weapons at a rate of about 3-5 weapons per year.
- ▶ Thirty percent of North Korea's total stocks of plutonium and weapon-grade uranium are assessed as in production pipelines, lost during processing, or held in a reserve.

North Korea keeps secret the number of nuclear weapons which it has built, and there is little, if any, reliable public information about this value. The above range of 13-30 nuclear weapons as of the end of 2016, based on the estimates of North Korea's production and use of plutonium and WGU, is an assessment.

North Korea may have a handful of plutonium-based warheads for its Nodong ballistic missile.



**CBRNE-TERRORISM NEWSLETTER – August 2017**

One uncertainty is judging North Korea's dependence on plutonium for its deployed nuclear weapons. It would have incentives to be able to build miniaturized, reliable weapons with only a weapon-grade uranium core, as its declaration after the September 2016 test could suggest it has done.

North Korea would have an incentive to build more advanced nuclear weapons. One type is a composite core nuclear weapon made from both plutonium and weapon-grade uranium. How many it may have built is unknown, as is their size, weight, and reliability. North Korea has enough plutonium for up to twelve nuclear weapons using a composite core of plutonium and weapon-grade uranium, where likewise 70 percent of the fissile material is utilized in the weapons themselves. However, North Korea is unlikely to build only composite core weapons. This estimate would suggest that North Korea could build several of them in addition to other types of nuclear weapons as well.

It is unknown whether North Korea could mount a warhead on a Nodong that uses only weapon-grade uranium or has a composite core. In particular, are they too large for the Nodong? However, both possibilities appear increasingly likely.

It is uncertain, and there are reasons to doubt, that North Korea can yet build reliable, survivable warheads for ICBMs.

Continued underground testing will provide North Korea opportunities to improve significantly its weapons in terms of less fissile material (particularly plutonium) per weapon, increased warhead miniaturization, and/or greater explosive yields.

Developing thermonuclear weapons, which can achieve all three above goals, is a declared priority of North Korea.

It appears capable of developing thermonuclear weapons. It is far more likely to be working on one-stage thermonuclear weapons rather than traditional two stage thermonuclear weapons, or "H-Bombs." The Institute does not assess North Korea as yet capable of building two stage thermonuclear weapons or utilizing gaseous mixtures of deuterium and tritium in a U.S.-style boosted fission weapon. However, North Korea is assessed as able to handle solid forms of lithium-6, deuterium, and/or tritium, such as those used in one-stage thermonuclear weapons or other types of boosted fission weapons.

Its existing knowledge should allow it to continue to make progress on a variety of deliverable nuclear weapons, even in the absence of additional underground nuclear tests.

**Through 2020**

Through 2020, North Korea is projected to have 25-50 (rounded) nuclear weapons.

A worst case, involving the operation of the Experimental Light Water Reactor (ELWR) at Yongbyon, is that it would have up to 60 nuclear weapons by the end of 2020.

In regards to composite core nuclear weapons, it would have enough plutonium for up to 17-32 nuclear weapons, where the above worst case including the ELWR determines the upper bound.

Significantly higher estimates are possible, such as one that is in an earlier 2015 Institute study on North Korean nuclear explosive materials, if North Korea significantly expands its gas centrifuge program and dramatically boosts its production and separation of plutonium over what is assumed in the current analysis.

— See David Albright, [\*North Korea's Nuclear Capabilities: A Fresh Look\*](#) (Institute for Science and International Security, 22 April 2017).





ICI  
International  
**CBRNE**  
INSTITUTE



# EXPLOSIVE NEWS



## Narco-Terror: Mexican Cartel Begins Using IEDs

By Brandon Darby

Source: <http://www.breitbart.com/texas/2017/07/23/narco-terror-mexican-cartel-begins-using-ieds/>

July 23 – Mexican intelligence services are sounding the alarm about one of Mexico's most violent cartels turning to the use of improvised explosive devices (IEDs) as part of their terrorist-style tactics.

A leaked report from Mexico's intelligence service CISEN revealed the ruthless Cartel Jalisco Nueva Generacion (CJNG) has turned to the recruitment of former terrorists from Colombia and their use of explosives and tactics, Mexico's [Excelsior](#) reported. The terrorist turned cartel mercenaries come from the far left terrorist organization once known as Revolutionary Armed Forces of Colombia or FARC. Since FARC and the Colombian government reached a cease fire, former guerrilla fighters made their way to Mexico and turned into cartel mercenaries where criminal organizations are actively seeking trained enforcers.

The intelligence report warns Mexican military and law enforcement forces to change their tactics when dealing with the CJNG to counter the terrorist tactics used by the FARC. One of the tactics that CISEN warns about in particular is the use of a particular type of improvised explosive device or IED commonly called a potato or "papa" for their unique shape.

With the capture and extradition of Sinaloa Cartel top boss Joaquin "El Chapo" Guzman Loera, his criminal empire fell into disarray through infighting and the attack of rival cartels. The power vacuum opened the door for CJNG to move in as one of the top criminal organizations. Once known as the Mata Zetas or Zeta Killers, the [CJNG began as an offshoot of the Sinaloa Cartel](#). The group eventually broke off and expanded into the worldwide market, Breitbart Texas reported. The once unknown CJNG has earned a reputation for being one of the most violent criminal organizations in Mexico. The cartel faced off against military forces, killing dozens of soldiers and police officers as well as shooting down helicopters. The criminal organization has also resorted to strapping explosives on their victims and setting them off on videotaped warnings to their rivals.

By working the European and Asian markets, the CJNG initially managed to keep a lower profile than Sinaloa which has drawn most the attention from the U.S. Drug Enforcement Administration over [their dominance of the heroin and opioid distribution](#) and the ensuing overdose epidemic that has swept the nation, Breitbart Texas reported.

*Ildefonso Ortiz is an award-winning journalist with Breitbart Texas. He co-founded the Cartel Chronicles project with Brandon Darby and Stephen K. Bannon. You can follow him on [Twitter](#) and on [Facebook](#).*

*Brandon Darby is managing director and editor-in-chief of Breitbart Texas. He co-founded the Cartel Chronicles project with Ildefonso Ortiz and Stephen K. Bannon.*

## FBI releases 'unusual' analysis of pipe bomb found in man's apartment after Bixby Air Force recruiting office bombing

Source: [http://www.tulsaworld.com/news/courts/fbi-releases-unusual-analysis-of-pipe-bomb-found-in-man/article\\_7c78ae4a-0266-570b-8993-859fec8ccf0e.html](http://www.tulsaworld.com/news/courts/fbi-releases-unusual-analysis-of-pipe-bomb-found-in-man/article_7c78ae4a-0266-570b-8993-859fec8ccf0e.html)

July 18 – An unexploded pipe bomb found in the apartment of a man jailed in connection with the bombing of a Bixby military recruiting office had unusual features, according to court records.

A preliminary Federal Bureau of Investigation analysis of one of two unexploded improvised explosive devices found in Benjamin Roden's south Tulsa apartment determined the device utilized two 9-volt batteries and magnets in its construction, a government affidavit states.

"FBI bomb technicians noted the nature of the IED was unusual for Oklahoma, because IEDs with these features are typically seen in other parts of the world," according to the affidavit, filed Monday in Tulsa federal court in support of a request for a search warrant.

Roden, 28, has been jailed since July 11, about 14 hours after a pipe bomb exploded in front of an unoccupied Air Force recruiting station at 10425 S. 82nd East Ave. in Bixby.

Roden is being held on two counts of destruction of federal property, malicious damage to federal property by use of explosive and use of explosive to commit a federal felony.





**CBRNE-TERRORISM NEWSLETTER – August 2017**

Investigators, with the help of a witness to the bombing and mail sent anonymously to an Oklahoma Air National Guard base in Tulsa, quickly developed Roden as a suspect.

Roden, a former Air Force senior airman trained as a firefighter, was discharged in April from the Oklahoma Air National Guard, according to a spokeswoman for the 138th Fighter Wing in Tulsa.

Roden joined the Air National Guard in 2014 after he left the Air Force, the spokeswoman said. He joined the Air Force in 2012.

Air Force officials told investigators that Roden resigned from active duty Air Force when he could not complete the training to become a certified electrician. He has since been described by other military personnel as “smart” and capable of building electronic devices, but also hateful of the military.

Acting U.S. Attorney Loretta Radford said last week that the bombing was not being characterized as domestic terrorism, but she added that the investigation was ongoing.

The description of the unexploded pipe bomb is contained in an application for a search warrant filed Monday in Tulsa federal court. The search warrant application indicates that officials are seeking evidence from Roden’s Google-associated accounts.

An affidavit filed by an FBI special agent in support of the search warrant application asks a judge to require Google Inc. to disclose to the government copies of records linked to Roden’s Gmail and YouTube accounts. Google owns YouTube.

The affidavit mentions a YouTube channel that contains three how-to videos uploaded one year ago that feature Roden as the instructor.

On the videos, Roden is seen giving instructions on how to build a thermostat. Another video depicts Roden building a light that can automatically switch on when placed in the dark.

A judge on Friday ordered Roden to undergo two independent mental exams after his public defender raised concerns about his ability to assist in his defense.

U.S. Magistrate Frank McCarthy scheduled a competency hearing for Roden on Aug. 29. McCarthy will hold a preliminary hearing and detention hearing for Roden the same day.

## Homemade bomb items readily sold

Source: <http://www.thestar.com.my/news/nation/2017/07/15/homemade-bomb-items-readily-sold/>



DIY: Many of the ingredients for a pipe bomb or even a small ammonium nitrate-fuel oil explosive are easily sourced.





**CBRNE-TERRORISM NEWSLETTER – August 2017**

July 15 – The incident where a homemade bomb was placed under the car of a nurse in Kapar on Sunday is a wake-up call on how easy it is to make an improvised explosive device (IED).

In fact, making your own explosives is easy enough via numerous videos and text instructions floating around the Internet.

Selangor CID chief Senior Asst Comm Fadzil Ahmat said it was alarming that information to make IEDs was easily accessible on the Internet.

"People can even view step-by-step instructions on YouTube.

"We are monitoring the situation, and no one should attempt to make their own bombs as they would end up in serious trouble," he told *The Star* yesterday.

Checks revealed that most materials for a homemade fertiliser bomb can be sourced from hardware stores.

The daily googled for the type of materials needed, and armed with a shopping list, managed to secure all of them within three hours.

They included a fertiliser used for household plants, batteries, wires, pipes and other items that were obtained for less than RM10 per piece. Materials needed to build a detonator, such as light bulbs and alarm clocks, could be sourced from convenience stores or shopping centres.

In total, less than RM80 was spent to purchase items for the homemade explosive.

The most difficult item to obtain was the fertiliser, which can be found at plant nurseries and farming supply businesses.

Checks with several plant nurseries in Seri Kembangan and Sungai Buloh showed that most have stopped selling fertiliser that can be used in an IED and have instead switched to organic fertilisers.

Still, it was not impossible to get a 1kg bag of the required fertiliser for about RM7 while a 50kg bag was going for about RM150 a piece.

A couple of traders *The Star* spoke to did not bat an eye when we asked for larger amounts of the fertiliser, which could then be used to make a car bomb.

## North Korea Launches Another Ballistic Missile

Source: <http://www.globalsecurity.org/wmd/library/news/dprk/2017/dprk-170728-voa01.htm>

July 28 – North Korea launched another intercontinental ballistic missile ((ICBM)) Friday, the second such launch in just a few weeks, the Pentagon said.

"We detected and tracked a single North Korea missile launch," Pentagon spokesman Navy Captain Jeff Davis told reporters. "We assess that this was an ICBM; this was a launch that had been expected."

Davis said North Korea launched the missile from Mupyong-ni arms plant in the country's north. He said it flew "in excess of 40 minutes" and traveled about 1,000 kilometers laterally before splashing down into the Sea of Japan, about 163 kilometers from Hokkaido, Japan's second-largest island.

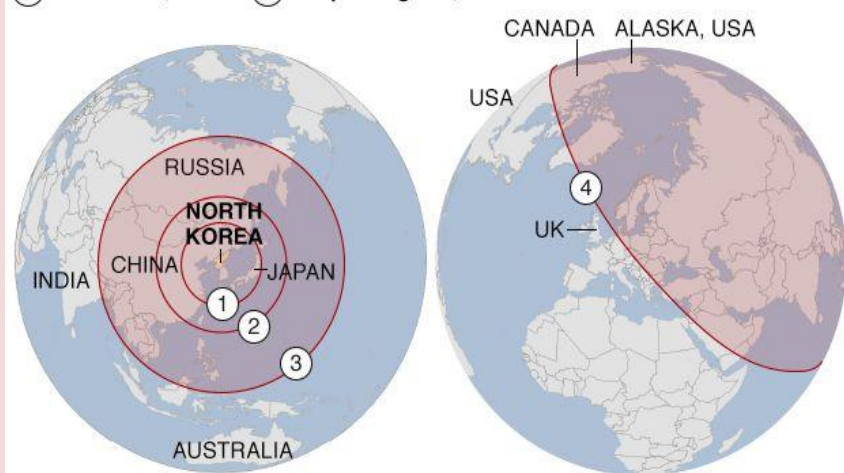
### Possible landing site

Japan's Prime Minister Shinzo Abe said the missile may have landed in that country's exclusive economic zone, and he convened an emergency meeting with Japanese officials to respond to the launch.

### North Korean missile ranges

Maximum estimated/calculated

- ① Nodong 1,300km
- ② Taepodong 1 2,000km
- ③ Musudan 4,000km
- ④ Taepodong 2 8,000km



**CBRNE-TERRORISM NEWSLETTER – August 2017**

Davis said the United States remains "as committed as ever to the defense of our allies, especially the Republic of Korea and Japan, in the face of these threats." He added the missile did not pose a threat to North America.

North Korea has carried out several ballistic missile tests over the past two years. Earlier this month, Pyongyang launched an intercontinental ballistic missile for the first time. The missile flew for 39 minutes and landed in the Sea of Japan. Experts said the ICBM may have had a range capable of reaching the U.S. state of Alaska.

"North Korea is slowly morphing into a nuclear and missile power right before our very eyes," said Harry Kazianis, director of defense studies from the Center for the National Interest.

After Friday's launch, the top U.S. general, Chairman of the Joint Chiefs of Staff Gen. Joseph Dunford, and the head of U.S. Pacific Command, Admiral Harry Harris, called the Republic of Korea's Joint Chiefs of Staff Chairman, General Lee Sun Jin. The U.S. Chairman's office said the military leaders discussed military response options and reaffirmed their "ironclad commitment" to the U.S.-Republic of Korea alliance.

Susan Thornton, the acting assistant secretary of state for East Asian and Pacific affairs, testified on Capitol Hill Thursday that North Korea is "the most urgent and dangerous threat."

"We are working to isolate and increase pressure on North Korea with the goal of convincing the regime to return to serious talks aimed at denuclearization. This has been and remains this Administration's top diplomatic priority," said Thornton.

## North Korean missiles can reach major U.S. cities beyond West Coast

Source: <http://www.homelandsecuritynewswire.com/dr20170731-north-korean-missiles-can-reach-major-u-s-cities-beyond-west-coast>

July 31 – Based on current information, the recent missile test by North Korea could easily reach the U.S. West Coast and a number of major U.S. cities.

UCS [notes](#) that news reports say that North Korea again launched its missile on a very highly lofted trajectory, which allowed the missile to fall in the Sea of Japan rather than overflying Japan. It appears the ground range of the test was around 1,000 km (600 miles), which put it in or close to Japanese territorial waters. [Reports](#) also say the maximum altitude of the launch was 3,700 km (2,300 miles) with a flight time of about 47 minutes.

If those numbers are correct, the missile flown on a standard trajectory would have a range 10,400 km (6,500 miles), not taking into account the Earth's rotation.

However, the rotation of the Earth increases the range of missiles fired eastward, depending on their direction. Calculating the range of the missile in the direction of some major U.S. cities gives the approximate results, shown in this table:

City	Distance from NK	Range of missile toward city
Los Angeles	9,500 km (5,900 mi)	11,700 km (7,250 mi)
Denver	9,800 km (6,100 mi)	11,400 km (7,100 mi)
Chicago	10,400 km (6,500 mi)	11,100 km (6,900 mi)
Boston	10,750 km (6,700 mi)	10,750 km (6,700 mi)
New York	10,850 km (6,750 mi)	10,850 km (6,750 mi)
Washington, D.C.	11,000 km (6,850 mi)	10,900 km (6,800 mi)



**CBRNE-TERRORISM NEWSLETTER – August 2017**

The table shows that Los Angeles, Denver, and Chicago appear to be well within range of this missile, and that Boston and New York may be just within range. Washington, D.C., may be just out of range.

USC notes that it is important to keep in mind that we do not know the mass of the payload the missile carried on this test. If it was lighter than the actual warhead the missile would carry, the ranges would be shorter than those estimated above.

## **New optical device detects drugs, bomb-making chemicals**

Source: <http://www.homelandsecuritynewswire.com/dr20170801-new-optical-device-detects-drugs-bombmaking-chemicals>

Aug 01 – Scientists searching for traces of drugs, bomb-making components, and other chemicals often shine light on the materials they're analyzing.

This approach is known as spectroscopy, and it involves studying how light interacts with trace amounts of matter.

One of the more effective types of spectroscopy is infrared absorption spectroscopy, which scientists use to sleuth out performance-enhancing drugs in blood samples and tiny particles of explosives in the air.

While infrared absorption spectroscopy has improved greatly in the last 100 years, researchers are still working to make the technology more sensitive, inexpensive and versatile. Buffalo says that anew light-trapping sensor, developed by a University at Buffalo-led team of engineers and described in an *Advanced Optical Materials* study, makes progress in all three areas.

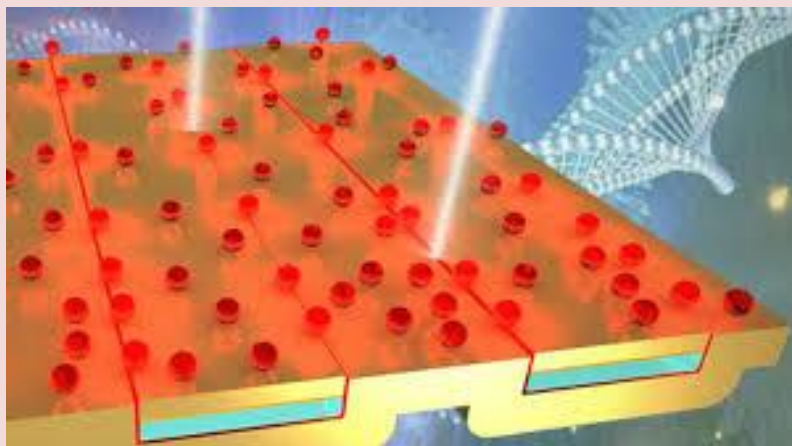
"This new optical device has the potential to improve our abilities to detect all sorts of biological and chemical samples," says Qiaoqiang Gan, PhD, associate professor of electrical engineering in the School of Engineering and Applied Sciences at UB, and the study's lead author.

Co-authors of the study — which will be featured on the cover of September's *Advanced Science News* — in Gan's lab include Dengxin Ji, Alec Cheney, Nan Zhang Haomin Song and Xie Zeng, Ph.D. Additional co-authors come from Fudan University and Northeastern University, both in China, and the University of Wisconsin-Madison.

**The sensor works with light in the mid-infrared band of the electromagnetic spectrum. This part of the spectrum is used for most remote controls, night-vision and other applications.**

**The sensor consists of two layers of metal with an insulator sandwiched in between. Using a fabrication technique called atomic layer deposition, researchers created a device with gaps less than five nanometers (a human hair is roughly 75,000 nanometers in diameter) between two metal layers. Importantly, these gaps enable the sensor to absorb up to 81 percent of infrared light, a significant improvement from the 3 percent that similar devices absorb.**

The process is known as surface-enhanced infrared absorption (SEIRA) spectroscopy. The sensor, which acts as a substrate for the materials being examined, boosts the sensitivity of SEIRA devices to detect



molecules at 100 to 1,000 times greater resolution than previously reported results.

The increase makes **SEIRA spectroscopy** comparable to another type of spectroscopic analysis, surface-enhanced Raman spectroscopy (SERS), which measures light scattering as opposed to absorption.

The SEIRA

advancement could be useful in any scenario that calls for finding traces of molecules, says Ji, the first author and a PhD candidate in Gan's lab. This includes but is not limited to drug detection in blood, bomb-making materials, fraudulent art and tracking diseases.





**CBRNE-TERRORISM NEWSLETTER – August 2017**

Researchers plan to continue the research, and examine how to combine the SEIRA advancement with cutting-edge SERS.

— Read more in Dengxin Ji et al., “Efficient Mid-Infrared Light Confinement within Sub-5-nm Gaps for Extreme Field Enhancement,” *Advanced Optical Materials* (3 July 2017).

## Royal Marine Commando made 14 pipe bombs and set off four in Northern Ireland

Source: <http://www.mirror.co.uk/news/uk-news/royal-marine-commando-made-14-10876933>

July 26 – A rogue Royal Marine with links to dissident republican groups made 14 pipe bombs - four of them deployed in northern Ireland, a court heard yesterday.



Ciaran Maxwell, 31, had a library of terror documents, bought chemicals and components and made bombs, which he stashed in England and Northern Ireland. The 31-year-old had maps, plans and lists of terror targets - as well as images of an adapted Police Service



Northern Ireland pass card and a PSNI uniform. The serviceman, who is originally from Larne, Co Antrim, pleaded guilty at the Old Bailey to preparation of terror acts between January 2011 and August last year.

At the beginning of a three-day sentencing hearing at the same court, prosecutor Richard Whittam QC, said: “Across 14 of the locations involved in the investigation, Mr Maxwell had in his possession, or had constructed, 14 pipe bombs.”

He added: “Of those 14 pipe bombs constructed by Mr Maxwell, four have been deployed in Northern Ireland.”

The court heard Maxwell was a serving Royal Marine Commando at the time of the offences, having enlisted on September 27 2010.

He joined 40 Commando at Norton Manor Camp in Taunton the following year and although he served in the UK and the United States never served in Northern Ireland.

Mr Whittam said: “Between 1 January 2011 and 24 August 2016, Mr Maxwell researched the manufacture and construction of explosives, acquired the items he needed to make explosive devices and constructed the devices.



**CBRNE-TERRORISM NEWSLETTER – August 2017**

“He stored the items he needed to make the devices, the devices themselves, ammunition, weapons, tools and resources in hides across England and Northern Ireland .

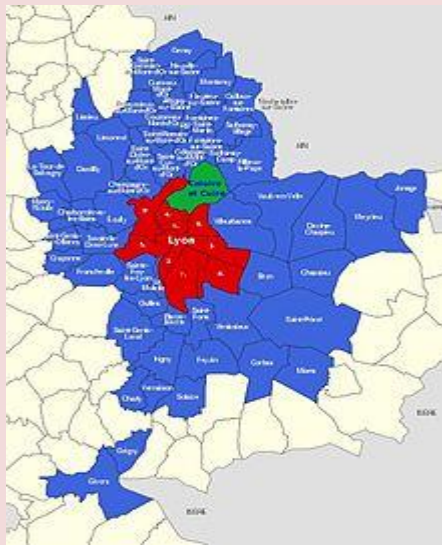
“He engaged in research to create of a library of maps, plans and lists of potential targets for a terrorist attack.”

The court heard he had hoarded more materials and chemicals to make explosives, as well as a replica handgun and ammunition.

Mr Whittam explained how a walker stumbled on one of Maxwell’s weapons caches in Carnfunnock Country Park, near Larne, in March last year.

He said: “It is our case that some of the items inevitably must have been taken from the UK to Northern Ireland by this defendant and it may be that, when travelling between England and the UK, bearing in mind the identity cards he would have had and his position, his passage would have been easier than others to take items with him.”

Maxwell appeared in court by video link from Woodhill prison in Milton Keynes, where he sat at a desk with a laptop and took notes.



## Rocket Launcher found next to Quranic School in France

Source: <https://megynkelly.org/364276/rocket-launcher-found-next-to-quranic-school-in-france/>

Aug 04 – A rocket launcher was discovered by chance this morning in an abandoned warehouse in Caluire-et-Cuire. This demilitarized material was located in the immediate vicinity of a building that had until recently housed a Koranic school. Caluire et Cuire is the fifth-largest suburb of the **city of Lyon**. The **Muslim school** was run by the Association Nouvel Horizon. It ceased operations in May. The founder and former director of the school was arrested and placed in custody to attend the searches. His school was adjacent to the building where the rocket launcher was found.

## Bombs Explode at Spanish Embassy in Caracas

Source <https://www.voanews.com/a/bombs-explode-spanish-embassy-venezuela/3972061.html>

Aug 05 – The Spanish embassy in Venezuela has been hit by explosive devices lobbed by two people on a motorcyc le, according to the Associated Press.



Prosecutors reported the incident Thursday, describing the explosives as gasoline bombs. There is no word on whether anyone was killed or injured.

Meanwhile, the first meeting of the 545



delegates elected to rewrite the constitution is set for Friday at the legislative palace in Caracas, setting the stage for a possible showdown





**CBRNE-TERRORISM NEWSLETTER – August 2017**

between President Nicolas Maduro and the political opposition, which says the election of the constituent assembly was not fair.

Opposition leaders are calling for a mass protest Friday.

"The only way they'll get us out of here is by killing us," said opposition spokesman Freddy Guevara.

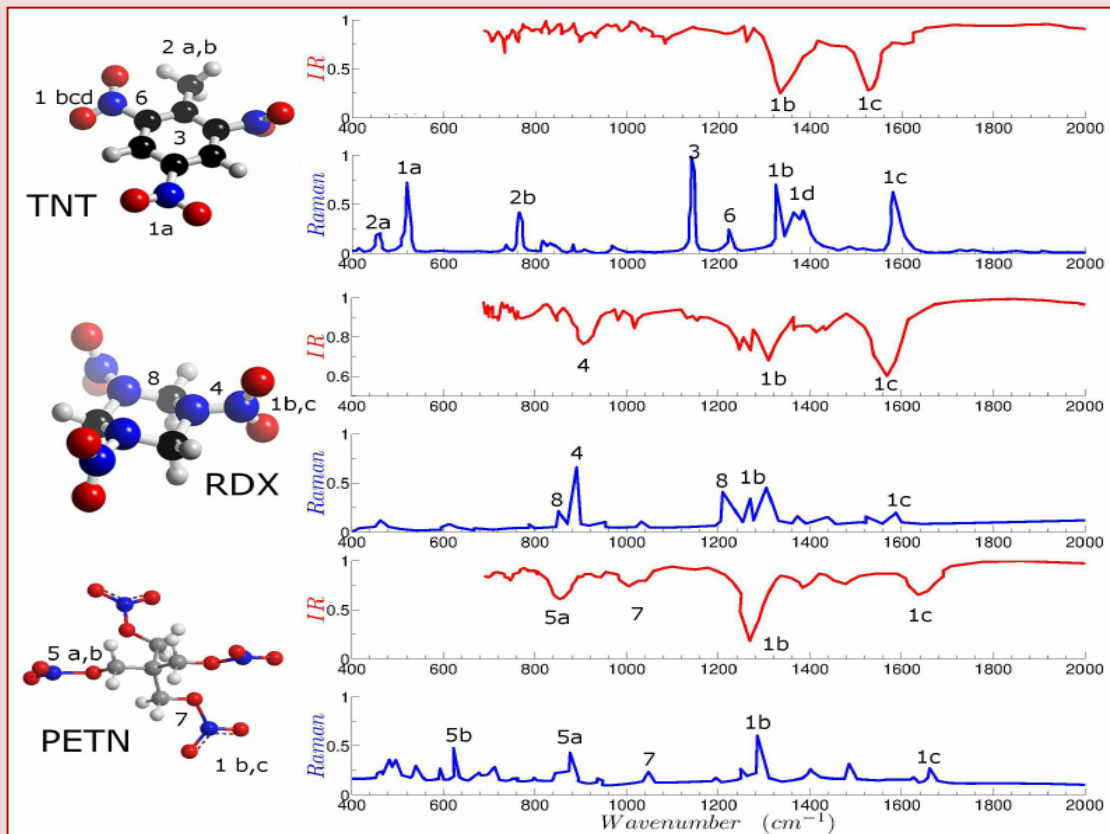
"They will never have the seat that the people of Venezuela gave us."

Freddy Guevara, first Vice-President of the National Assembly and lawmaker of the Venezuelan coalition of opposition parties (MUD), attends a session of Venezuela's opposition-controlled National Assembly in Caracas, Venezuela, Aug. 2, 2017.

## A New Resolution for Explosive Detection

Source: <http://i-hls.com/archives/77896>

Aug 04 – Scientists are developing new methods to reveal traces of drugs and bomb-making components. A rather new approach named spectroscopy and in particular, infrared absorption spectroscopy, is used by scientists to detect performance-enhancing drugs in blood samples and tiny particles of explosives in the air. While the method has improved greatly in the last 100 years, researchers are still working to make the technology more sensitive, inexpensive and versatile.



Infrared and Raman spectra of explosives

A new light-trapping sensor, developed by a University of Buffalo-led team of engineers, makes progress in all three areas. "This new optical device has the potential to improve our abilities to detect all sorts of biological and chemical samples," Qiaoqiang Gan, PhD., associate professor of electrical engineering in the School of Engineering and Applied Sciences at UB told the University's site.

The sensor works with light in the mid-infrared band of the electromagnetic spectrum. This part of the spectrum is used usually for remote controls, night-vision and other applications.

The sensor consists of two layers of metal with an insulator sandwiched in between. Using a fabrication technique called atomic layer deposition, researchers created a device with gaps less than five nanometers between two metal layers. The gaps enable the sensor to





**CBRNE-TERRORISM NEWSLETTER – August 2017**

absorb up to 81 percent of infrared light, a significant improvement from the 3 percent that similar devices absorb.

The device, **SEIRA** (Surface Enhanced Infrared Absorption Spectroscopy), is a great advancement and could be useful in any scenario that calls for finding traces of molecules, says Ji, the first author and a PhD. candidate in Gan's lab. This includes, but is not limited to, drug detection in blood, bomb-making materials, fraudulent art and tracking diseases. Researchers plan to continue the research, and examine how to combine the SEIRA advancement.

The research is supported by the U.S. National Science Foundation's Nanomanufacturing program, the National Science Foundation of China and the Chinese Scholarship Council.

## **Passenger with pipe bomb allowed to fly after staff failed to spot device was dangerous**

Source: <http://www.telegraph.co.uk/news/2017/07/31/passenger-jet-bomb-man-allowed-fly-airport-security-failed-spot/>



July 31 – n airline passenger who tried to carry a “crude but viable” nail bomb onto a Ryanair plane was released and allowed to catch a later flight because security staff did not realise the device was dangerous, a court heard yesterday.

Nadeem Muhammad, 43, was stopped after airport scanners detected the makeshift device as he tried to board a plane from Manchester international airport to Bergamo near Milan in January this year.

But swabs of the device failed to detect any explosives and Muhammad was released after questioning and allowed to return to his home in Bury, Greater Manchester.

Five days later he was allowed to board another Ryanair flight to Italy and was only arrested on his return after new forensic tests showed the device was explosive, Manchester Crown Court was told.

The 43-year-old from Bury appeared at Manchester Crown Court on Monday charged with possession of an improvised pipe bomb made of an explosive propellant in the barrel of a marker pen which also contained pins.

The explosive was linked to three domestic batteries and wires which would complete a circuit and explode the device when joined.

Muhammad, who is originally from Pakistan, but holds an Italian passport, denies possession of the bomb with intent to endanger life and a lesser alternative charge of possession of the bomb in suspicious circumstances.

Jonathan Sandiford, prosecuting, said the device was found in a green suitcase when it passed through security scanners at the airport in January this year.



**CBRNE-TERRORISM NEWSLETTER – August 2017**

He said: "It is a matter of common sense that the only reason he would have tried to get that device onto the aeroplane was that he intended to detonate it in the confines of the Boeing 737, endangering the lives of the passengers on board and causing damage to the aircraft itself."

The court heard an X-ray scanner showed three batteries with wires going into the barrel of a marker pen which also contained pins among the explosive powder.

The case was diverted for further checks and the device was found zipped in lining. A security worker quizzed Muhammad who said he did not know what it was and his wife or other unknown persons must have put it in the case.

He was also questioned by the airport's counter terror unit, but swabs of the device failed to detect any explosive substance and officers formed the view that it was not a viable device.

**The device was confiscated and he was allowed to return home after the police had confirmed his identity.**

Five days later he boarded a flight to Bergamo for an 11 day stay.

But the device was then further examined by a forensic expert who "immediately suspected it was more sinister".

It was sent for specialist investigation to a laboratory in Kent where another expert concluded it was an "unreliable, unpredictable but viable device."

Mr Sandiford said: "The fact that it was badly designed or constructed and was unreliable does not change the central fact that it was intended to be used as an improvised explosive device."

"The only reason anyone would try to smuggle that device through stringent security checks was because he had the desire and intention to cause injury and possible death."

The trial continues.

## **India: Armymen slip into anti-mine boots**

Source: <http://www.dnaindia.com/india/report-now-armymen-slip-into-anti-mine-boots-2521254>

Aug 06 – Scientists at the International Advanced Research Centre for Powder Metallurgy and New Materials (ARCI), the R&D centre for the Department of Science and Technology, have developed special boots that deflect the impact of a blast from an Improvised Explosive Device (IED) or landmine, the biggest killer for service personnel. The soles of these shoes are made of ceramic in a honeycomb structure.

IED blasts have claimed the lives of a large number of security personnel over the years. According to National Bomb Data Centre data, from 2012 to 2016, 1,143 IED bomb blasts or landmine blasts have taken place across the country, claiming the lives of 2,663 security personnel.

The Indian Army has procured these specially-designed boots from ARCI, and are using them in landmine-affected areas.

**"Normal boots do not safeguard security personnel against landmine blasts. But, if we replace the soles of the shoes with ceramic, it helps absorb heat from mines, and will cause less injuries. Also, the honeycomb design of the sole also absorbs heat," said a scientist from ARCI who was part of the project.**

The ARCI plans to make these boots available to paramilitary forces as well, considering a large number are concentrated in naxal-affected areas, where landmine blasts are common.

## **Afghan Officials Seize Truck With 16 Tons Of Explosives**

Source: <https://www.rferl.org/a/afghanistan-truck-explosives-seized/28661479.html>

Aug 06 – Afghan intelligence officials said on August 6 that they had seized a truck in Kabul carrying more than 16 tons of explosives hidden in boxes marked as poultry feed.

The National Directorate of Security said in a statement that the truck had Pakistani license plates, adding that five people were arrested.

"It was loaded with explosives to make bombs, suicide vests and conduct terrorist activities in Kabul," the statement said, adding that 16,500 kilograms of explosives was seized.





**CBRNE-TERRORISM NEWSLETTER – August 2017**

On May 31, a massive truck bomb ripped through the Afghan capital's diplomatic quarter during the



morning rush hour, killing about 150 and wounding around 400 people, mostly civilians.

No group claimed responsibility for the attack that was caused by over 1,500 kilos of explosives hidden in a sewage truck, according to Western officials.

Taliban militants have intensified their attacks since they launched their "spring offensive" in late April, with civilians bearing the brunt of the conflict.

**The United Nations estimates that more than 26,500 civilians have died and nearly 49,000 have been injured as a result of armed conflict in Afghanistan since January 2009.**

## **Bomb squad sent in over chemicals at Newcastle College**

Source: <http://news.sky.com/story/bomb-squad-sent-in-over-chemicals-at-newcastle-college-10976645>



Aug 06 – A bomb disposal unit has carried out a controlled explosion at Newcastle College following concerns over the storage of chemicals.

Roads were cordoned off while Army officers moved the substances from the city centre campus to be blown up on Town Moor.

The soldiers were called in after a member of staff raised concerns.





**CBRNE-TERRORISM NEWSLETTER – August 2017**

It followed advice issued nationally about the storage of particular chemicals used at schools and colleges. Residents near the campus were not evacuated but were informed about the incident.

Chief Inspector Dave Morrison said there was "nothing untoward or suspicious about this incident".

"A diligent member of staff raised concern and, as a precaution, the chemicals were disposed of safely by explosives ordnance disposal," he said.

"I'd like to thank local residents and people in the area for their patience and understanding while emergency services dealt with the incident as we appreciate there will have been some disruption for them."

## **'How many times has this happened?' Border force faces questions over 'terror bomb' mailed from Turkey**

Source: <http://www.smh.com.au/federal-politics/political-news/how-many-times-has-this-happened-border-force-faces-questions-over-terror-bomb-mailed-from-turkey-20170804-gxpqtw.html>

Aug 04 – Border and security authorities would be "doing a lot of soul searching" following revelations that a bomb kit was allegedly [mailed to Australia by the Islamic State](#) and probably couldn't be sure that more explosive devices had not come into the country, a leading expert has said.

After the Australian Federal Police revealed that the bomb at the centre of the alleged Sydney plane terror plot had been sent by air cargo from Turkey, a spokeswoman from the Department of Immigration and Border Protection said that the scale of mail and air cargo "presents a unique challenge".

John Coyne, a former AFP transnational crime specialist now with the Australian Strategic Policy Institute, said that it was impossible to check all items of cargo and mail coming into Australia. Authorities would not know whether other such devices had been sent to Australia.

"A question now will be what other devices were sent through, how many, who to?" Dr Coyne said. "That will be a worrying issue in many people's minds in domestic and international security. Is this the first time this has happened? How many times has it happened? There is no way of telling."

He said the explosives used in the Manchester attack on an Ariana Grande concert could just have easily been sent by mail.

"My experience is, let me assure you, there'll be a lot of soul-searching around targeting at borders. Can we use big-data analytics, explosive detection, can we make it more affordable? What are the cost and time implications? There will be a range of questions government will be going through."

## **Raven's Challenge Exercise Promotes Interoperability**

Source: <https://www.defense.gov/news/article/article/1267174/ravens-challenge-exercise-promotes-interoperability/>

Aug 03 – "Help, I've got a bomb strapped to me!" the hostage yelled to the explosive ordnance disposal technician as he gingerly stepped over a booby-trapped victim to approach the hostage on the stairs.



Air Force Staff Sgt. Brandon Ulmer, left, and Merl Mireles, an investigator with Orange County Sheriff's Department in California, prepare a controlled small blast firing device during the Raven's Challenge explosive ordnance disposal exercise at Camp Pendleton, Calif., Aug. 1, 2017. Raven's Challenge is an Army-funded exercise led by the Bureau of Alcohol, Tobacco, Firearms, and Explosives with support and participations from multiple federal, state and local agencies. DoD photo by EJ Hersom



**CBRNE-TERRORISM NEWSLETTER – August 2017**

This is just one of the many realistic scenarios U.S. and Belgian service members and federal, state and local public safety bomb squads face during the [Raven's Challenge](#) XI exercise here this week.

Raven's Challenge is an international full-scale, live-fire, counter-improvised-explosive-device interoperability exercise that presents participating military EOD technicians and civilian public safety bomb squads with the opportunity to coalesce as a team, develop a plan and respond to an IED problem set, said John Simpson, Raven's Challenge exercise program manager. Simpson served in the Army as an EOD technician for 22 years and has been with the Bureau of Alcohol, Tobacco, Firearms and Explosives in Atlanta for 15 years.

**Exchanging Ideas and Methods**

Exercises like Raven's Challenge are important because it increases the interoperability between the military and law enforcement agencies to meet domestic threats, such as the 2013 Boston Marathon bombing, Simpson said. "This is the perfect exercise to have the military and public safety bomb squads training together and working together before another Boston occurs," said Don Robinson, special agent in charge with the ATF's National Center for Explosives Training and Research in Huntsville, Alabama. "We run these exercises so they can exchange ideas, get familiar with each other's tactics, techniques and procedures and equipment, and just familiarize them with each other and how each side's going to perform its mission.

"They're finding out how long it takes to get things approved and how long it takes procedures to happen on each side here for the first time instead of in the real world in a real situation," he said. "They bring so much experience, but they're getting that crossover that they wouldn't get at home station."

**Different Tools**

Col. David Schmitt, chief of the Army's counter-IED EOD solutions division at the Pentagon, said the best part about military EOD technicians training at Raven's Challenge training with ATF, FBI and public safety bomb squads is that they can each learn new tactics, techniques and procedures, known as TTPs -- from each other and establish connections. "We include the federal agencies and military together. That provides ... a rich depth of

knowledge, because you've got some guys who have spent 20 years in the military and then gone on to work in the federal agencies and have been doing this for decades," he said.

Many military EOD technicians have experience with IEDs in Iraq, Afghanistan and other places that the public safety bomb squads may not have seen, he noted. "And then you have some of the other scenarios, like the hostage situation -- military service members don't normally respond to something like that, but civilian bomb squads would normally train for that kind of scenario, so they may have more experience with that kind of thing."

An exercise scenario in which military EOD technicians use night-vision goggles while disarming devices in a dark warehouse allows them to share their experiences and equipment, Schmitt added.

Chief Master Sgt. Douglas Moore, the Air Force's EOD career field manager at the Pentagon, said exercises like Raven's Challenge are essential for the interoperability training of the EOD enlisted force.

"Today, we have about 60 percent of our EOD airmen who've never deployed. We've turned over our active duty force relatively significantly, as well as our total force with the Guard and Reserve, so to bring all of those folks here to share information, look at some of the different environments and get training is important," he said.

**Domestic Situations**

"We want to make sure we're not just focusing on combat operations," he continued, "and that's what Raven's Challenge is doing. It's focusing on the domestic IED conventional operations as well, because we have to take different things into account when we're operating in those kinds of environments."

Army Staff Sgt. Sean Mattes said he and the other EOD technicians assigned to Fort Bliss, Texas, train with the El Paso bomb squad, the Border Patrol, the Drug Enforcement Administration, the Transportation Security Administration and the FBI.

"I can't tell you how many different times we've been doing something with another service or another police department, and they've said, 'Hey, I've got another way of doing that,' and they do it," said Army Spc. Seth Hamilton. "And the same thing goes for them. They're doing something, and it's like, 'I can fix



**CBRNE-TERRORISM NEWSLETTER – August 2017**

that for you real quick' and you go over there and fix it right up. The biggest thing about these [exercises] is making things not only faster, but safer, safer, safer. So many different ideas are being thrown around out there, and it's awesome. You can't get it anywhere else."

One example of a domestic operation any of the EOD technicians would face is a local police department or public safety bomb squad seeking help with unexploded ordnance such as a World War II souvenir a veteran has in his home or yard.

Al Carbonara has been with the Los Angeles Police Department bomb squad for 21 years. If his officers respond to a military ordnance situation, he said, they try to take care of it first, and call their military counterparts if they can't. "People don't realize how much military ordnance is out there or how many meth labs," he said. "People are making stuff, making homemade fireworks, things like that. ... I got called out 14 times last week alone."

**Military-Civil Cooperation**

Air Force Tech. Sgt. Michael Ault, an EOD technician from Travis Air Force Base, California, said it's common for older veterans to have unexploded ordnance. "At our home station, we get called about once a week for various UXO calls, and then we have responded

to various different suspected IEDs and things like that," he said.

Air Force Senior Airman Alex Nona, another EOD technician from Travis, said his team attends monthly meetings with the Sacramento- and San Francisco-area bomb technicians and host training at their proficiency range.

"We go and do training with them, so we kind of know each other, so when they call up on the phone, it's not us calling the police department. We're talking to the bomb squad, and we know the people on the squads," he said. "It's really important to know who you're working with and to know how they operate. They know what we have, and we know what they don't have, so we can always go and support them."

Air Force Staff Sgt. Darrell Linkus, an Air National Guard EOD technician from Buckley Air Force Base, Colorado, is a firefighter with the Westminster Fire Department as well. Because he is a guardsman and firefighter, he said, he works closely with his law enforcement counterparts in Colorado in the Denver area.

"It's good to be able to work with these guys -- see their TTPs, they can see our TTPs -- and it's something we can bring back, that interoperability with law enforcement and military EOD. It makes us work better together," he said.

**Greece – EOD Police dog retired**

**Ελληνική Αστυνομία**  
@hellenicpolice

Ακολουθήστε

Σε ευχαριστούμε BLANCO για τις Υπηρεσίες σου! 🐕👮  
Ο συνεργάτης μας BLANCO, τ. Αστυν. Σκύλος Ανίχν. Εκρηκτ.  
Υλών, "συνταξιοδοτήθηκε" προσφάτως  
12:30 μ.μ. - 14 Αυγ 2017

4 53 261



Hellenic Police  
Thank you BLANCO for your  
Services!  
Our partner BLANCO – former Police  
EOD Dog was recently retired!





## AQAP Chief Bomb Maker Al-Asiri Calls For Attacks On Transport Systems In The U.S. In Issue 17 Of English-Language 'Inspire' Magazine

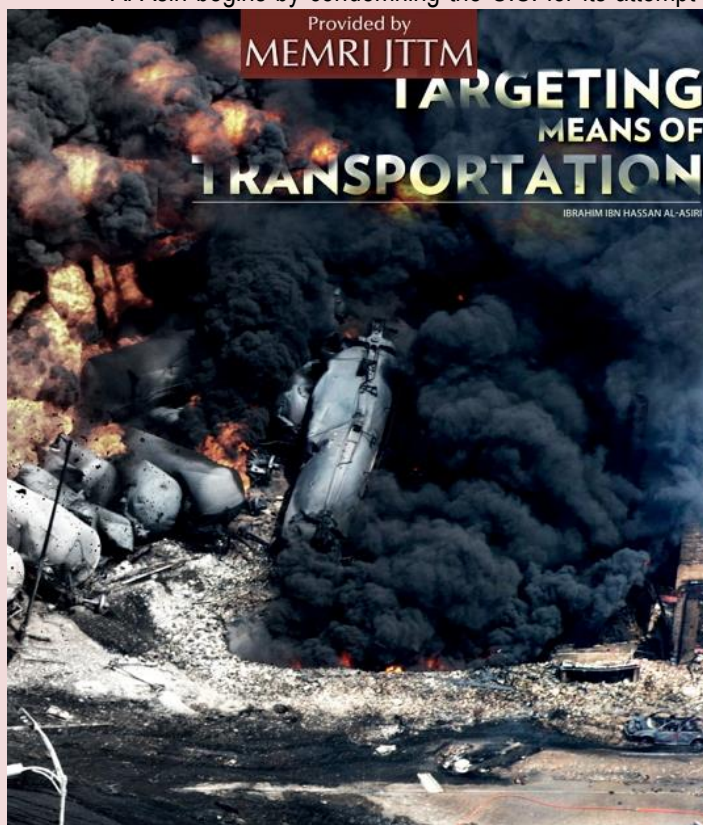
Source: <https://www.memri.org/jtm/aqap-chief-bomb-maker-al-asiri-calls-attacks-transport-systems-us-issue-17-english-language>

Aug 14 – An article by Al-Qaeda in the Arabian Peninsula's (AQAP) chief bomb maker, Ibrahim Al-Asiri, in Issue 17 of the organization's magazine *Inspire*, titled "Targeting Means of Transportation," calls to target American transport systems (ground, air and sea transportation for both passengers and freight), stressing that they are a prime target because attacks on them undermine public security and also cause great economic harm by scaring away tourists and investors. Moreover, says the article, such attacks are easy even for lone operatives to carry out, since there are many targets and the security measure around them are easily overcome.<sup>[1]</sup>

It should be noted that the article was apparently written during Barack Obama's presidency, because Al-Asiri refers to him and his policies and does not mention President Trump.

Following are excerpts from the article:

Al-Asiri begins by condemning the U.S. for its attempt to export its values. He especially mentions the



affirmation of gay rights, and the celebration of these by president Obama's administration: "America started spreading its culture and ideals across the globe via the mass media, press and the internet. Sugar-coating these values with attractive names such as justice, freedom and equality, in order to make them much more appealing to people. But, as the days pass and through globalization itself, the reality of these values were exposed. What was once being propagated as 'good values' in the media became apparent to all; thanks to globalization itself. America's justice was exposed in Afghanistan, Iraq and other areas where masses of innocent people were killed because of its 'justice'. Another face of America's morals and values revealed itself in the form of laws legislated to legalize sexual deviation as a proud American value. When a president comes out joyfully to proudly legislate these perversions, lighting up the walls of the Whitehouse with their perverted rainbow symbols indicating that they have adopted these morals. This collapse in morals and values, which is generally rejected in

nature, all religions and denied by medical doctors and psychologists; has exposed the concealed nature of globalization and the reality of American democratic values."

Al-Asiri goes on to say that AQAP intends to target the U.S. security, which is the weak link in the chain of U.S. dominance. Undermining security is relatively easy for lone jihadis, he says: "As for us, we will be focusing on targeting means of transportation. We will explain more on this, which is part of the general policy of targeting the ring of security in the chain... When referring to transportation we refer to air, sea and ground transportation - both local and international. Jihad groups and organizations may have the ability to target international means of transportation. As for the Lone Mujahid, his abilities may be limited to targeting internal means of transportation of a country. And it is possible for him to draw a comprehensive plan so as to execute such kind of operations..."



**CBRNE-TERRORISM NEWSLETTER – August 2017**

He goes on to stress the importance of trains in the U.S., especially freight trains: "In America, trains are considered to be among the most important means of transportation within the country i.e. between cities and its outskirts, and from one city to another, especially when transporting freight. Normal busses, trams and trolley busses are used in Europe and America for transportation within the cities and its outskirts. All these means of transportation indicate that the world and the civilian life are very dependant on them. And what becomes apparent is that it is too difficult to protect these means of transportation. And here is where we find its vulnerability – means of transportation today are considered to be a weak point which we must focus on..."

Al-Asiri points out that attacks on public transportation can be done in three ways: by targeting the vehicle itself; its route or track; and its stations, terminals or transit points. He goes on to explain the effects of such attacks, first and foremost causing terror among the population:

**"The following are the effects and consequences caused by targeting means of transportation, either directly or indirectly:**

1. There will be a state of terror, fear and lack of security among the masses. And this is because of: a. The targeted areas are public infrastructure, used by people from all classes and walks of life at all times. The daily routine surrounding it makes it impossible to be rid of. b. The large numbers and numerous types of means of transportation will always set an environment of looming danger everywhere. c. Difficult to cover all security loopholes. Doing so will mean halting all the necessary daily civilian activities, such procedures might be the same as security measures placed during pandemics. d. The existence of tough security measures in all public arenas and the transportation sector increases the feeling of insecurity and fear among the people. This is because in cases of emergency and increased searches, security officers deal with people in a manner that make them feel a sense of danger and therefore makes them respond to these tough procedures placed by the government by being extra cautious and take quick precautions to inform the government in cases of any real threat. It is no doubt that all these create an environment of fear.

2. These operations will damage the security of the economy by directly exhausting the economy. Here are some important points that explain the causes of the exhaustion of the economy. a. The security measures that would be placed so as to cover the loophole which allowed an operation to succeed in the first place. These measures include increase in security forces and labor hours, purchasing sophisticated equipment, establishing new special units to specifically face these threats and reinforcing counter intelligence efforts to disrupt any attempt of another attack whatsoever. b. Insurance companies increase their rates with the increase in risk. c. Loss incurred in the target vehicle itself (Train, airplane etc.), E.g. The cost of a single plane is millions of dollars. d. Some transport companies may get into bankruptcy if targeted regularly and are unable to secure themselves, this will make people seize using such a company for their transportation needs. These are the most important consequences that may accompany these kind of operations."

The article lists the following advantages of targeting transport systems: " 1. Means of transportation have extensive and multiple targets that are widespread and open to access with varying degree of security, increasing the opportunity for a successful operation. 2. The capability to infiltrate the security measures placed by all means of transportation. With little resources, it is possible to achieve great results, this is, if the operations is well executed and planned. 3. The results of these kind [sic] of operations are disastrous to the economy, especially if they occur regularly. 4. Gives the Lone Mujahid the ability to carry out a large scale operation using these types of small resourced operations. 5. It is difficult for the authorities to secure all security loopholes in these operations. 6. The ability to use different kinds of weapons, and ways to subdue the enemy according to the conditions and circumstances at hand."

Al-Asiri concludes by calling on Al-Qaeda followers and "mujahideen" to target America: "After this quick review, in which we show the importance of focusing on specific kinds of targets, I urge my Mujahideen brothers everywhere, especially the Lone Jihad heroes; I say to them: Target America, by Allah they are in a great predicament. They cannot get out of it and cannot find real solutions to its problems beyond its borders. We see them laying alternative plans to their wars in Afghanistan, Iraq and other places; making alliances after being unable to fight the war all alone. This state of weakness appears clearly in one of Obama's speeches, in which he said 'globalization is still standing'. Trying to imply that America is still a dominant power. What makes Obama declare this is the weakness that is overshadowing America. The U.S. laid a fifteen-year plan in which it raised the debt, lowered interest rates and reduced military expenditure, which will continue for many years



to come. America today is refreshing its efforts to revive its economy. And we should continue to focus our efforts against it until the world gets rid of this international system led by America, and until Muslims enjoy freedom to practice their faith, freedom to apply the Laws of Allah and until Muslims secure themselves, wealth and resources from the hands of America."

[1] Source: Telegram.me/ Akhbar Qa'edat Al-Jihad fi Jazirat Al-'Arab, August 13, 2017.

## 'Bomb Italian ships!' Shock as Libyan general THREATENS Italy over migrant rules

Source: <http://pamelageller.com/2017/08/bomb-italian-ships.html/>

Aug 04 – Libya has ordered its military to bomb Italian ships in a shocking threat to naval fleets heading to the coast to help with the migrant crisis.

The Italian government authorised the country's navy to carry out the mission on Wednesday, in a bid to stop refugees crossing the Mediterranean sea and heading to Europe.



But the presence of Italian ships in Libyan waters provoked furious reactions from the north African country.

And General Khalifa Haftar, who controls most of the east of Libya, ordered his forces to bomb any ships engaged in the upcoming naval support mission according to a tweet by news site Al Arabiya.

The tweet read: "#Haftar orders bombing of #Italian warships requested by Sarraj."

Gen Haftar's forces are thought to be unlikely to open fire on the naval rescue mission ships.

But the threat could further complicate the already delicate project and further strain relations between the general and the country's UN-backed government in Tripoli. The Libyan National Army said in a statement: "Commander-in-Chief of the armed forces, Field Marshal Khalifa Haftar, issues orders to the Libyan naval bases in Tobruk, Benghazi, Ras Lanuf and Tripoli to confront any marine unit that enters the Libyan waters without the permission of the army."

The order comes a few hours after Libya's parliament in Tobruk also expressed its

opposition to the Italian naval operation.

Ministers claimed the problem with the agreement for joint action to fight human traffickers is that Libya believes the presence of foreign ships would be a "violation of their national sovereignty". The shocking warning comes after two Italian fishing boats were attacked by a vessel in Zarsis, off the border between Libya and Tunisia, in international waters. The boat, which apparently belonged to the Tunisian customs authorities, desisted and left.

Italy agreed initially to deploy two ships, in the operation to help the Libyan coastguard and target people smugglers. The Italian Defence Minister Roberta Pinotti said there would be "no harm done or slight given to Libyan sovereignty", before stressing the mission would not be a "blockade" preventing migrant boats from leaving. More than 94,000 migrants have crossed the Mediterranean to Italy so far this year according to the UN – a record number.





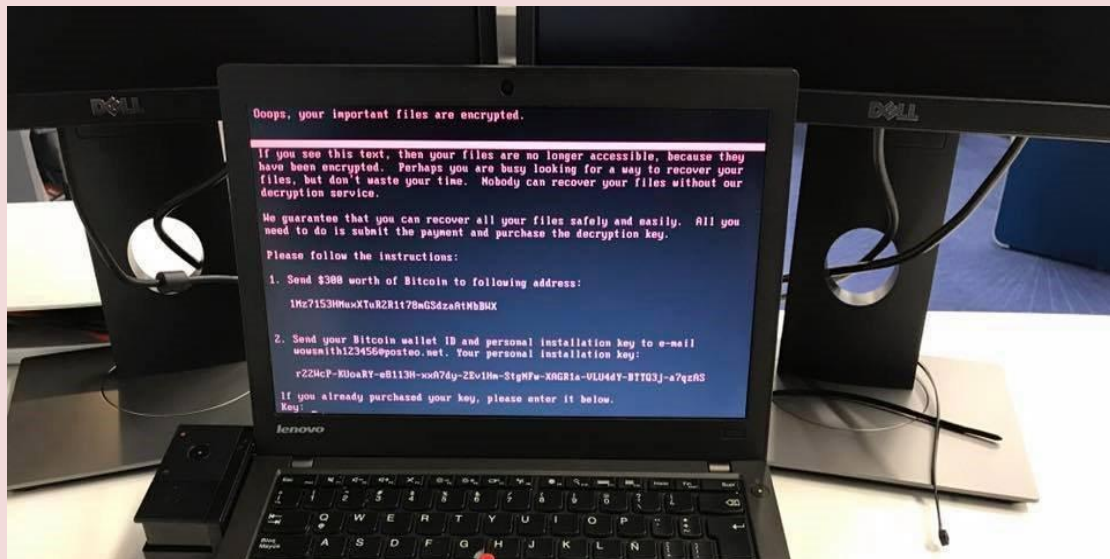


# CYBER NEWS



## Petya variant hobbles European businesses

Source: <http://www.homelandsecuritynewswire.com/dr20170725-petya-variant-hobbles-european-businesses>



July 25 – In the wake of May's WannaCry attack, which affected more than 230,000 computers in over 150 countries, a fast-moving malware [malware](#) outbreak was [reported](#) 27 June at targets in Spain, France, Ukraine, Russia, and other countries. The attack [infected](#) large banks, law firms, shipping companies, and even the [Chernobyl nuclear facility](#) in the Ukraine. As with WannaCry, [hackers employed](#) malicious software using the EternalBlue vulnerability in older Microsoft Windows systems to rapidly spread across an organization. The [new malware](#) is thought to be a variant of Petya, a wiper malware designed to destroy systems and data with no hope of recovery.

"This new malware, dubbed Petya—or NotPetya, as it seems to be a completely new form of malware—is far more destructive than WannaCry," says Timothy Crosby, Senior Security Consultant for [Spohn Security Solutions](#). "The motivation behind WannaCry seems to have been merely financial, while the Petya variant aimed to create widespread system destruction where data was not as easily recovered." In addition, the Petya variant corrupts the MBR (master boot record) and MFT (master file table), making complete system restoration incredibly difficult—if not impossible—for those infected.

Using EternalBlue, both WannaCry and the Petya variant exploit a vulnerability in the SMB (server message block) data transfer protocol used to share files and printers across local

networks. WannaCry, a [traditional form of malware](#), resides on a computer or device in the form of files, either embedded in or masquerading as non-malicious files. After the WannaCry attack, Microsoft released a patch for the SMB vulnerability. However, the Petya variant [goes a step further](#) by employing two additional ways of spreading rapidly within an organization, by targeting a network's administrator tools. So, if the SMB route failed, the Petya variant is able to harvest credentials from the infected system and, using PsExec and WMIC administrative tools, gain access to other systems on the network.

Malware, such as the malicious software used in the Petya variant attacks, is growing increasingly sophisticated, employing techniques that are not easily remediated. Fileless malware, for instance, resides in areas not normally scanned, such as in RAM (random access memory) or even the operating system kernel itself. Because it does not rely on files in order to run, propagate and accomplish its purpose, fileless malware is virtually impossible to detect using standard [cyber security](#).

"To remediate in a NotPetya-like situation, a cyber security team must be vigilant about the activity on the network," advises Crosby. "Security teams should monitor for aberrant and unexpected behavior, such as accounts being used at odd hours, at multiple locations or while on vacation." To prevent permanent damage to data and network systems,





businesses should employ a host of protection programs that notify personnel when a threat exists.<sup>7</sup> This includes Security Information and Event Management (SIEM) systems that automatically aggregate events and alerts based on anomalous activity. These programs can [mitigate risk](#) by halting the spread of ransomware throughout the entire network and alerting IT when malware is attempting to contact external resources that store the keys used to encrypt files.

Crosby adds that most attacks can be easily prevented by following a few simple rules. First, use only supported versions of windows (Windows 7 and Server 2008 are the oldest supported versions as of this date). Ensure that antivirus software is up-to-date and fully patched. Remind employees to not open any files received from unknown sources. And, lastly, back-up computers regularly, keeping backup files off-site.

## U.S. weapons main source of trade in illegal arms on the Dark Web

Source: <http://www.homelandsecuritynewswire.com/dr20170726-u-s-weapons-main-source-of-trade-in-illegal-arms-on-the-dark-web>

July 26 – Sixty percent of weapons on sale on the “dark web” are from the United States, according to a new study – [Behind the Curtain: the illicit trade of firearms, explosives and ammunition on the dark web](#). The report states that Europe is the source of around 25 percent of weapons on sale on the dark web. However, transactions of weapons sold to European customers on the dark web generate estimated revenues that are around five times higher than those sold to U.S. customers.

The study from the not-for-profit research organization [RAND Europe](#) and Judith Aldridge, Professor of Criminology at the University of Manchester, is the first piece of research exploring the size and scope of the illicit trade of firearms, explosives and ammunition on the dark web.

RAND [notes](#) that the study involved data collection on the dark web between 19–25 September 2016, which covered 12 cryptomarkets, a type of dark web marketplace that brings together multiple sellers managed by marketplace administrators, and 167,693 listings. From these listings, 811 were identified as relevant for the purpose of the study.

The dark web was found to facilitate the illegal sales of firearms, weapons, explosives and banned digital products that provide guides on “home-made” explosives and weapons. Findings from the study suggest that the dark web is increasing the availability of better performing, more recent firearms for the same, or lower, price, than what would be available on the street or the black market.

Despite being unlikely to fuel large-scale terrorist operations and armed conflicts, the study illustrates how the dark web has the potential to become the platform of choice for individuals (for example, “lone-wolf” terrorists) or small groups (for example, gangs) to obtain weapons and ammunition. The lone-wolf terrorist attacker in the [2016 Munich shooting](#) used weapons purchased on the dark web.

[Giacomo Persi Paoli](#), the report’s lead author and a research leader at RAND Europe, says, “The dark web is both an enabler for the trade of illegal weapons already on the black market and a potential source of diversion for weapons legally owned. Recent high-profile cases have shown that the threat posed by individuals or small groups obtaining weapons illegally from the dark web is real. The ability to not only arm criminals and terrorists, who can make virtually anonymous purchases, but also vulnerable and fixated individuals is perhaps the most dangerous aspect.”

Judith Aldridge, Professor of Criminology at the University of Manchester and a co-investigator on the research, says, “In very simple terms, anyone can connect to the dark web and within minutes have access to a variety of vendors offering their products, which are most often illegal. The dark web enables illegal trade at a global level, removing some of the geographical barriers between vendors and buyers, while increasing the personal safety of both buyers and sellers through a series of anonymizing features that obscure their identities. This veil of anonymity, combined with the relative ease of access, makes the dark web an attractive option for a wide range of sellers.”

Forty-two percent of the 811 arms-related listings on cryptomarkets were for firearms, followed by arms-related digital products (27 percent) and others, including ammunition (22 percent). Pistols were the most commonly listed firearm (84 percent), followed by rifles (10 percent) and sub-machine guns (6 percent).





**CBRNE-TERRORISM NEWSLETTER – August 2017**

The trade in arms-related digital products poses complex challenges. These products are often guides that provide tutorials for a wide range of illegal actions, ranging from the conversion of replica/alarm guns into live weapons, to the full manufacture of home-made guns and explosives, and also include models that can be turned into fully-working firearms through 3D printing.

The overall value of the arms trade based on the twelve cryptomarkets analyzed in the study is estimated to be in the region of \$80,000 per month, with firearms generating nearly 90 percent of all these estimated revenues. Every month there could be up to 136 untraced firearms or associated products in the offline world that have been traded on the dark web. However, estimates of the arms trade on cryptomarkets, in terms of both value and volume, will include a certain percentage of fake listings or transactions.

Persi Paoli says, “The arms trade on the dark web is a drop in the ocean compared to the legal trade of arms worldwide. However, compared to other products traded on the dark web, the numbers are not necessarily the most appropriate indicator of how serious the issue is. A few people using illegally purchased weapons from the dark web can have severe consequences.”

He continues, “We’re unable to ascertain the extent of scamming, but know this occurs across all product categories on dark web markets, and perhaps more frequently for vendors of firearms. Despite the uncertainty, we should not dismiss or play down the threat posed by the arms trafficking phenomenon on the dark web.”

The illegal sales of weapons on the dark web present challenges for law enforcement agencies and national governments. These challenges largely derive from the anonymity enabled by the dark web, which makes identifying individuals and linking them to specific activities challenging.

However, Persi Paoli believes that governments and law enforcement agencies can use existing measures to tackle illegal arms trafficking to limit the dark web trade. He says, “The dark web offers a platform to trade firearms, but does not create completely new firearms. If properly implemented, all measures designed to tackle illegal arms trafficking ‘in the real world’ may reduce the availability of illegal weapons to be traded. The only exception is the availability of 3D models for home-made 3D-printed firearms on the dark web. This new element will require further investigation as 3D printing continues to develop and grow.”

Persi Paoli concludes, “The emergence of the dark web as an enabler for arms trafficking certainly requires appropriate responses at all levels. However, this does not mean that existing measures should be considered obsolete.”

**In brief****Findings**

- ◆ The dark web is an enabler for the circulation of illegal weapons already on the black market, as well as a potential source of diversion for legally owned weapons.
- ◆ The dark web is increasing the availability of better performing, more recent firearms for the same, or lower, price, than what would be available on the street on the black market.
- ◆ The United States appears to be the most common source country for arms that are for sale on the dark web. Almost 60 percent of the firearms listings are associated with products that originate from the United States. This is followed by a selection of European countries, which account for roughly 25 per cent, while unspecified locations of origin account for roughly 12 percent. However, Europe represents the largest market for arms trade on the dark web, generating revenues that are around five times higher than the United States.
- ◆ Firearms listings (42 percent) were the most common listings on the dark web, followed by arms-related digital products (27 percent) and others, including ammunition (22 percent). Pistols were the most commonly listed firearm (84 percent), followed by rifles (10 percent) and sub-machine guns (6 percent).
- ◆ The trade in arms-related digital products poses additional complex challenges. These products are often guides that provide tutorials for a wide range of illegal actions, ranging from the conversion of replica/alarm guns into live weapons, to the full manufacture of home-made guns and explosives, and also include models that can be turned into fully-working firearms through 3D printing.
- ◆ The overall value of the arms trade on the dark web based on the 12 cryptomarkets analysed in the study is estimated to be in the region of \$80,000 per month, with firearms generating nearly 90 percent of all revenue. Due to the arms trade on the dark web, every



**CBRNE-TERRORISM NEWSLETTER – August 2017**

month there could be up to 136 untraced firearms or associated products in the real world.

- ◆ Estimates on the value and volume of the arms trade on the dark web may include a certain percentage of fake listings or transactions, particularly among vendors of firearms. However, it is challenging to ascertain the extent of scamming on the dark web.
- ◆ The dark web is unlikely to be the method of choice to fuel conflicts because arms are not traded at a large enough scale and due to the potential limitations on infrastructure and services in a conflict zone. On the other hand, the dark web has the potential to become the platform of choice for individuals (for example, lone-wolves terrorists) or small groups (for example, gangs) to obtain weapons and ammunition behind the anonymity curtain provided by the dark web. In addition, the dark web could be used by vulnerable and fixated individuals to purchase firearms.
- ◆ The illegal arms trade presents further challenges for law enforcement agencies and national governments. These challenges largely derive from the anonymity of individuals that use the dark web to purchase arms.

**Final remarks and observations**

- ◆ The dark web introduces a new platform enabling arms trafficking at a global scale. Despite the relatively limited value and volume of weapons traded on the dark web compared to either other products type (for example, drugs) or to equivalent products trafficked offline, the potential impact on internal security is significant as demonstrated by recent “lone-wolf” terrorist attacks in Europe.
- ◆ The development of the dark web will require policy makers and law enforcement agencies to adapt intervention strategies, ensure that proper regulatory frameworks are in place, ensure that adequate resources are made available and ensure that specialist skills are developed.
- ◆ The dark web does not produce new weapons; it merely acts as an enabler of trafficking, with weapons and ammunition having to be shipped and delivered in the “real world.” Therefore, good traditional policing and investigative techniques will remain vital in responding to this threat. In addition, traditional firearms control measures designed to tackle illicit trafficking remain of the outmost importance to reduce the availability of illegal firearms. These include efficient marking and record keeping practices, international cooperation for tracing, and good stockpile management.
- ◆ Existing international instruments for combating arms trafficking should not be considered obsolete. The validity of some instruments should certainly be examined and perhaps require amendments, but the emergence of a new threat does not necessarily require the creation of new instruments.
- ◆ The study represents the first attempt to collect and analyze primary data related to the sale of firearms and related products on the dark web. In order to generate a more robust understanding of the role of the dark web in enabling arms trafficking, a more continuous monitoring activity should be implemented. This would involve repeating and refining the data collection and analysis presented in this study over time in order to generate historical data that can be used to analyze trends. This would also involve a more rigorous assessment of the validity and applicability of current national and international counter-arms trafficking regimes, including policies, laws and regulations, actors and resources.

**Silicon Valley Censorship**

By Sam Westrop

Source: <http://www.meforum.org/6844/silicon-valley-censorship>

July 26 – Google's latest project is an application called Perspective, which, as [Wired reports](#), brings the tech company "a step closer to its goal of helping to foster troll-free discussion online, and filtering out the abusive comments that silence vulnerable voices." In other words, Google is teaching computers how to censor.

If Google's plans are not quite Orwellian enough for you, the practical results are rather more frightening.

Released in February, Perspective's partners include the *New York Times*, the *Guardian*, *Wikipedia* and the *Economist*. Google, whose motto is "Do the Right Thing," is aiming its bowdlerism at public comment sections on newspaper websites, but the potential is far broader.



**CBRNE-TERRORISM NEWSLETTER – August 2017**

Perspective works by identifying the "toxicity level" of comments published online. Google [states](#) that Perspective will enable companies to "sort comments more effectively, or allow readers to more easily find relevant information." [Perspective's demonstration website](#) currently allows anyone to measure the "toxicity" of a word or phrase, according to its algorithm. What, then, constitutes a "toxic" comment?

The organization with which I work, the Middle East Forum, studies Islamism. We work to tackle the threat

<p>88% likely to be perceived as "toxic"</p> <p>Radical Islam is a problem</p>	SEEM WRONG?
<p>87% likely to be perceived as "toxic"</p> <p>ISIS is a terrorist group</p>	SEEM WRONG?
<p>92% likely to be perceived as "toxic"</p> <p>Hamas's charter calls for killing Jews</p>	SEEM WRONG?

posed by both violent and non-violent Islamism, assisted by our Muslim allies. We believe that radical Islam is the problem and moderate Islam is the solution.

Statements rated as "toxic" by Google's Perspectives software

Perspective does not look fondly at our work -- see selections at left. No reasonable person could claim that saying "radical Islam is a problem" is hate speech. But the problem does not just extend to opinions.

Even factual statements are deemed to have a high rate of "toxicity." Google considers the statement "ISIS is a terrorist group" to have an 87% chance of being "perceived as toxic." Or 92% "toxicity" for stating the publicly-declared objective of the terrorist group, Hamas.

Google is quick to remind us that we may disagree with the result. It [explains](#) that, "It's still early days and we will get a lot of things wrong." The Perspective website even offers a "Seem Wrong?" button to provide feedback.

These disclaimers, however, are very much beside the point. If it is ever "toxic" to deem ISIS a terrorist organization, then -- regardless of whether that figure is the result of human bias or an under-developed algorithm -- the potential for abuse, and for widespread censorship, will always exist.

The problem lies with the very concept of the idea. Why does Silicon Valley believe it should decide what is valid speech and what is not?

Google is not the only technology company enamored with censorship. In June, Facebook [announced](#) its own plans to use artificial intelligence to identify and remove "terrorist content." These measures can [be easily circumvented](#) by actual terrorists, and how long will it be before that same artificial intelligence is used to remove content that Facebook staff find to be politically objectionable?

In fact, in May 2016, the "news curators" at Facebook [revealed](#) that they were ordered to "suppress news stories of interest to conservative readers from the social network's influential 'trending' news section." And in December 2016, Facebook [announced](#) it was working to "address the issue of fake news and hoaxes" published by its users. The *Washington Free Beacon* later [revealed](#) that Facebook was working with a group named Media Matters on this issue. In one of its own pitches to donors, Media Matters [declares](#) its dedication to fighting "serial misinformers and right-wing propagandists." The leaked Media Matters document states it is working to ensure that "Internet and social media platforms, like Google and Facebook, will no longer uncritically and without consequence host and enrich fake news sites and propagandists." Media Matters also [claims](#) to be working with Google.

Conservative news, it seems, is considered fake news. Liberals should oppose this dogma before their own news comes under attack. Again, the most serious problem with attempting to eliminate hate speech, fake news or terrorist content by censorship is not about the efficacy of the censorship; it is the very premise that is dangerous.

Under the guidance of faulty algorithms or prejudiced Silicon Valley programmers, when the *New York Times* starts to delete or automatically hide comments that criticize extremist clerics, or Facebook designates articles by anti-Islamist activists as "fake news," Islamists will prosper and moderate Muslims will suffer.





**CBRNE-TERRORISM NEWSLETTER – August 2017**

Silicon Valley has, in fact, already proven itself incapable of supporting moderate Islam. Since 2008, the Silicon Valley Community Foundation (SVCF) has granted \$330,524 to two Islamist organizations, the Council on American-Islamic Relations (CAIR) and Islamic Relief.

Both these groups are [designated](#) terrorist organizations in the United Arab Emirates. SVCF is America's largest community foundation, with [assets of over \\$8 billion](#). Its corporate partners [include](#) some of the country's biggest tech companies -- its [largest donation](#) was \$1.5 billion from Facebook founder Mark Zuckerberg. The SVCF is Silicon Valley.

In countries such as China, Silicon Valley has previously [collaborated](#) with the censors. At the very least, it did so because the laws of China forced it to comply. In the European Union, where freedom of expression is superseded by "the reputation and rights of others" and the criminalization of "hate speech" (even where there is no incitement to violence), Google was [ordered](#) to delete certain data from search results when a member of the public requests it, under Europe's "right to be forgotten" rules. Rightly, Google opposed the ruling, albeit unsuccessfully.

But in the United States, where freedom of speech enjoys protections found nowhere else in the world, Google and Facebook have not been forced to introduce censorship tools. They are not at the whim of paranoid despots or unthinking bureaucrats. Instead, Silicon Valley has *volunteered* to censor, and it has enlisted the help of politically partisan organizations to do so.

This kind of behavior sends a message. Earlier this year, Facebook [agreed](#) to send a team of staff to Pakistan, after the government asked both Facebook and Twitter to help put a stop to "blasphemous content" being published on the social media websites. In Pakistan, blasphemy is punishable by death. Google, Facebook and the rest of Silicon Valley are private companies. They can do with their data mostly whatever they want. The world's reliance on their near-monopoly over the exchange of information and the provision of services on the internet, however, means that mass-censorship is the inevitable corollary of technology companies' efforts to regulate news and opinion.

At a time when Americans have [little faith](#) in the mass media, Silicon Valley is now veering in a direction that will evoke similar ire. **If Americans did not trust the mass media before, what will they think once that same media is working with technology companies not just to report information Silicon Valley prefers, but to censor information it dislikes?**

*Sam Westrop is the director of Islamist Watch, a project of the Middle East Forum.*

## **Laptops, tablets, and all 'electronics larger than a cellphone' are now subjected to extra security measures for all passengers at US airports**

- TSA officers will order travelers to take all devices larger than a cellphone out of their bag and put them in a bin by themselves
- Prior rules required only laptops to be removed for separate screening
- Officials say it gives X-ray screeners a clearer picture of the devices

Source: <http://www.dailymail.co.uk/news/article-4732662/TSA-expands-new-procedure-inspecting-large-electronics.html>

## **Why can't films and TV accurately portray hackers?**

By By Kor Adana

Source <http://www.bbc.com/future/story/20170802-why-cant-films-and-tv-accurately-portray-hackers>

Aug 04 – In sixth grade, Mrs Minninger assigned our class an independent study project – give a presentation on any topic of our choosing. I chose hackers.



**CBRNE-TERRORISM NEWSLETTER – August 2017**

When it came time to present, I came across the same problem that producers and directors have been struggling with for almost 30 years now: How do I make hacking look interesting in a visual way?



Mr Robot focuses on Elliot, a cybersecurity engineer and hacker who finds himself in the midst of a 'hacktivist' plan to take down a huge corporation (Credit: USA Network)

I ended up showing the [war dialing clip](#) from the film WarGames and the ["Rabbit! Flu shot!" clip](#) from the film Hackers. (Years later, I referenced the same Hackers clip in season one of Mr Robot [when Mobley and Romero watch it in the hotel](#) on the way to [data security facility] Steel Mountain.)

At the end of my presentation, Mrs Minninger said, "That's not what real hacking looks like. That looks like a video game." She didn't know anything about network security, but she was right.

That was the mid-90s. Today, audiences are more sophisticated. They consist of real users who spend a great deal of time on their phones, tablets, and laptops. They have a better idea of what's possible and how the technology functions. We live in a world of ransomware attacks, predator drones, phishing scams, and data breaches that have the power to sway an election. As time goes on, it's becoming more difficult to get away with false portrayals of hacking and technology. Some of the most famous offenders are...

- [Swordfish](#) – John Travolta forces Hugh Jackman's character to hack into the Department of Defense in under 60 seconds. We see cheesy 3D visuals of viruses and authentication attempts.
- [Enemy of the State](#) – Jack Black's character looks at security footage and uses the cliché "zoom and enhance" function. Not only does he successfully zoom into the footage with no loss of picture quality, but he's able to somehow rotate the image in a 3D space.
- [Under Siege 2: Dark Territory](#) – Need to hack a computer? No worries. All it will take is a gigabyte of memory. That's all Eric Bogosian needs to get into a system. In the world of this movie, hacking is that easy.
- [NCIS](#) – Famously dubbed "2 idiots 1 keyboard," this is the most absurd and incorrect portrayal of computer usage, let alone hacking, that I've ever seen. Two agents furiously type on one keyboard at the same time in order to combat a hacker who's overtaking the system – all while flashy snippets of graphics and code strobe the screen.
- [Hackers](#) – This is probably one of the worst offenders when it comes to using video game graphics to represent hacking. We fly through 3D visualisations of data and encounter a singing virus that screams for help when it's being attacked.
- [GoldenEye](#) – Again, Alan Cumming's screen looks like a video game here. He uses a single command "send spike" and that's all it takes to break into a computer system.
- [Jurassic Park](#) – In the midst of a velociraptor attack, Ariana Richards sits down at a computer and says, "It's a Unix system. I know this." Then she somehow hacks the entire Jurassic Park security system in a matter of seconds and takes control of the automatic doors. This scene is filled with tension, but what she does is analogous to someone loading a browser on a Macbook and then saying, "It's Safari. I know this," and then going on to



compromise someone's Gmail account in a couple seconds. While most people troll this scene for its usage of 3D graphics on screen, she's actually using a real 3D filesystem called FSN.

### Special series: Cyber-hacks

This week, the BBC is taking a close look at all aspects of cyber-security. The coverage is timed to coincide with the two biggest shows in the security calendar - Black Hat and Def Con.

[Follow all the coverage via this link](#)

### Why does Hollywood get hacking so wrong?

There's an easy explanation for this trend. Most writers, directors, and producers believe that it's impossible to portray real hacking on screen and still have it be entertaining. (That's why you see the cheesy game-like graphics, skulls, and expository messages on screen.) I couldn't disagree more with this mindset.

If a scene needs flashy or inaccurate graphics on a computer in order to increase the drama or explain a plot point, there's an issue with the writing. On *Mr Robot*, we work hard to ensure that the stakes of the scene and the character motivations are clear even if you have no idea how the technology works. If you do understand the technology, you have the added bonus of recognising real vulnerabilities, real desktop environments, and authentic dialogue that fits the context of the hack.

A perfect example of this is the beginning of Episode Four in Season One, when Elliot explains his plan to hack into Steel Mountain. A layperson watching that scene understands that they need to break in somewhere and destroy some data – it will be risky, but it's necessary. A hacker watching that scene will recognise Elliot's accurate use of a Raspberry Pi and his plan to destroy the data sitting on archived LTO tapes by exploiting the HVAC system.

Most shows and films don't have a team dedicated to achieving this level of technical accuracy. On *Mr Robot*, the authenticity is incorporated into the outlining phase when we're fleshing out the stories – before we even start writing the scripts. When we're filming the series, we use practical screens with real code on them. We don't shoot green screens and "burn in" content in post-production. We use real software as often as possible.

I have an amazing team of hackers (Ryan Kazanciyan, Andre McGregor, James Plouffe) who consult on the show. We test each attack before it gets incorporated into the story. What sets us apart from the rest of these productions is the extra effort that goes into getting the little details right.

That grain of authenticity is a relief for the tech community, but it also resonates with the lay audience. People with no cybersecurity experience can intuit and judge the technical accuracy on screen; they say that our show *looks and sounds* real.

So thank you, Mrs Minninger, for inadvertently teaching me a lesson that would help shape my career: don't make it look like a video game.

[Kor Adana](#) is a writer/producer on USA Network's *Mr Robot*.

## Computer Expert that Stopped 'WannaCry' Global Cyberattack Arrested for Prior Cybercrimes

Source: <http://www.breitbart.com/tech/2017/08/04/computer-expert-that-stopped-wannacry-global-cyberattack-arrested-for-prior-cybercrimes/>

Aug 05 – The computer expert who managed to stop the WannaCry global cyberattack faces 40 years in jail over accusations he helped develop malicious software in 2014.

Marcus Hutchins, a 22-year-old man from England, was arrested at the Def Con hacking conference in Las Vegas last week on charges he helped to create and sell a malware tool that targeted bank accounts. "Hutchins, who was at a hacking conference in Las Vegas when he was arrested by the FBI, faces six counts of helping to create, spread and maintain the banking trojan Kronos between 2014 and 2015," reported [the Telegraph](#) on Friday. "According to the US Department of Justice indictment, the alleged offenses took place between July 2014 and July 2015. Hutchins was







jointly charged with another individual who was not named. The indictment alleged that Hutchins ‘created the Kronos malware’ and the other person later sold it for \$2,000 (£1,500) online.”

Hutchins was heralded as a hero after he managed to stop the WannaCry global cyberattack, which took place in May and targeted both private and public organizations, including the United Kingdom’s National Healthcare Service.

“The maximum statutory sentence he could face is decades, roughly 40 years,” claimed cyber criminal lawyer Tor Ekeland. “Would he get that? I doubt it, it would be a bizarre outcome. Is it possible? It sure is.”

“The main thing to do now is enter a not guilty plea as soon as you can, get him out on bail, and then you’ve got some breathing room,” continued Ekeland. “There’s not a single allegation that he made any money or anybody came to any harm from it. The indictment is very thin. It’s legally bizarre and there’s little detail.”

## Tracking terrorists online might invade your privacy

Source: <http://www.bbc.com/future/story/20170808-tracking-terrorists-online-might-invade-your-privacy?ocid=twfuT>

Aug 08 – Remember that picture you sent to your family of your children playing in the paddling pool? Or that private text you sent to someone trusted? Or when you searched for medical advice?

Then, guess what: those messages and websites you visited will be stored and could potentially be obtained by criminals. What’s more, as soon as these messages are sent, they could potentially be read by government agencies.



Protesting against overreaching surveillance online isn't new - this demonstrator took to the streets in Sofia, Hungary in 2010 (Credit: Getty Images)

That’s because the British government has rolled out the [Investigatory Powers Act](#) (known derisively to some as the Snooper’s Charter). It’s



**CBRNE-TERRORISM NEWSLETTER – August 2017**

gained new powers that now allow government agencies to access our online communications in real-time.

A draft technical capability notice was [leaked](#) in May to the [Open Rights Group](#), a civil rights group. Such a notice would legally compel a telecommunications firm to record all of the communications by the target(s) named in the warrant, and to transmit this information, in near real-time, in a readable format.

Following the recent terror attacks in London and Manchester, Prime Minister Theresa May reiterated her intention to “regulate cyberspace to prevent the spread of extremist and terrorism planning.”

This is to help protect us from future acts of terrorism – but is it an intrusion into our private lives?

### **Safety vs. privacy – which is more important?**

In the UK, the vast majority of the population support the prevention of terrorism: in 2010, a survey revealed that nine in 10 are happy with a proportionate loss of privacy in certain circumstances, such as full-body scanners in [airport security checks](#). And in 2015, [another survey](#) showed that double the amount of Americans were concerned the government wasn't doing enough to fight terrorism than the amount of Americans who were concerned with losing certain civil liberties in the process.

However, the Investigatory Powers Act goes beyond this, and the real-time aspect adds an extra level of danger.

The Act first came into effect on 29 November 2016. From that point, all telecommunication services were compelled to store records of all electronic communications and record people's internet browsing history, as well as, when served with a warrant, allow the government access to this information.

Now, information regarding every app, email, instant message, text, podcast, video and Skype call is recorded and stored, by service providers for up to a year. The document that was leaked earlier this year adds that this information could be transmitted in real-time.

Whilst the actual content of these communications is not stored, it is the associated metadata (who we speak to, where we were, when it took place and how long we spent talking) that is recorded. For intelligence agencies, this information can offer far more insight than the actual content of the communication.

The Investigatory Powers Act was enacted in order to protect against terrorist attacks, but the wide-reaching surveillance powers enshrined in this legislation has been likened by some to someone [accessing your phone](#). “Under the guise of counter-terrorism, the state has acquired totalitarian-style surveillance powers and this is the most intrusive system of any democracy in history,” says Silkie Carlo, senior

advocacy officer with [Liberty](#), a UK-based human rights watchdog group.

There is the argument of “Nothing to hide, nothing to fear”, in support of this mass surveillance. However, whilst we may have nothing to hide, we still have the right to a private life.

Unfortunately, in recent years, some have come to view ‘privacy’ as having something illicit to hide. Privacy may be a significant concern to people who are engaged in legal, but immoral activities, but all internet users should be concerned about the security of their data and safeguards against its misuse.

Others have argued that internet companies, like Facebook and Google, already have access to much of this data. However, we consent to this access in exchange for free use of their services, through accepting their terms and conditions.

The Investigatory Powers Act replaced the [Data Retention and Investigatory Powers Act](#) and expanded the surveillance powers to include all forms of communications. “It is legislating their existing powers so they could be regulated and there could be some oversight of what they are doing,” says Monica Horten, a visiting fellow for the [London School of Economics](#).

The blanket surveillance legislated by the Investigatory Powers Act formalises the intelligence services' ability to store and analyse the communications of the UK population for any possible crimes being committed. Through automated or manual analysis of our online behaviour, the intelligence services will be able to predict potential terrorists plotting new attacks.

“The interception [of online communications] exists, it is just a matter of putting things into formality, which is better, because you can have oversight and some level of judicial scrutiny,” says Yair Cohen, social media solicitor and author of [The Net is Closing: Birth of the e-police](#).

“Nobody is complaining when



terrorists are stopped because of interception.” However, blanket surveillance that harvests everyone’s data presents its own problems.

### Investigating criminals’ online info needs to be more precise

“The Draft Regulation Capability Notice does not tell us anything we didn’t know anyway when the bill went through,” says Ross Anderson, professor of security engineering at [Cambridge University](#). “They explicitly give the Home Secretary, specifically [Government Communications Headquarters](#), the power to serve arbitrary secret orders on technology firms. This is going to lead to serious trouble.”

One of the key aspects of the Investigatory Powers Act is that internet connection records will be stored for a year. Unlike browsing history, which records each webpage we have visited, the internet connection records are a history of each website visited.

This record of online behaviour provides telling information of who the subject is and what they do. Repeated visits to the NHS website would indicate a person with medical concerns, whilst visiting a particular bank indicates where they keep their money. “The amount of data they are collecting is quite a lot and the picture they can build up using the metadata is quite significant,” says Horten. “They can build up a picture of you and your lifestyle.”

The details of the security requirements are mandated in the technical capability notices, which are all confidential. However, the recent hacks of [TalkTalk](#) and [Yahoo](#), which saw millions of accounts leaked, highlighted failings within their network security. There have also been incidents where government laptops, containing highly sensitive information, have been [lost](#).

A repository of all our personal communications and details will naturally become a target for hackers.

### Private info motherlode

Using this stored information, criminals would be able to conduct increasingly personalised scams, targeting us based on our online habits. Scammers already pose as major banks and large companies, such as BT and Microsoft. Access to internet connection records would enable criminals to perform increasingly targeted scams against individuals, using information such as their favourite online stores

or which charities they support, in order to build trust and appear legitimate.

Now with the real-time access, scammers could be able to accurately reference recent online activities, making their fraudulent emails appear all that more legitimate.

The sheer amount of data that can now be collected is colossal. As of 2015, there were 65 million people living in the UK. As 90% of the UK population is using the internet, this means there will be 58.5 million records. “Even mathematically, it is an absolute certainty that you will generate false-positives if your starting point for surveillance is the entire population,” says Carlo.

The Investigatory Powers Act allows a broad number of government agencies access to the stored personal data. These range from agencies like the Metropolitan Police and the security services, through to the Food Standards Agency. There is also the question of who, within these agencies, would be able to view this information and how access to the information would be regulated and audited for potential misuse.

Edward Snowden, who leaked classified information from the National Security Agency (NSA) in 2013 was not an employee of the NSA, but a sub-contracted employee from Dell. Despite his status as an external subcontractor, Snowden was nonetheless able to leak the largest number of classified government documents ever in the history of the intelligence services. If Snowden was able to access this information, it is fair to ask what guarantees the public now have that similar incidents will not occur with their private data.

The Investigatory Powers Act also compels telecommunication companies to install government equipment at their premises, for the purposes of interception. Whether this equipment comes under the judicial review is unclear. “It is like the difference between the police getting a search warrant to search your home, and putting a policeman in to live as one of the family,” observes Horten.

In order to regulate its use, the Investigatory Powers Act includes a judicial double-lock, where a warrant is required for access, followed by judicial review. However, Liberty argues that this is only a single-lock. “The Judicial commissioner has to sign off the secretary of state or the police constables on a judicial review basis, which means they





**CBRNE-TERRORISM NEWSLETTER – August 2017**

are signing off a warrant on the basis that the correct procedure has been followed, rather than signing off a warrant on the basis of the facts,” says Carlo.

The European Court of Justice has argued that the indiscriminate collection of data was [against EU law](#). Liberty has also [gained high court](#)

[approval](#) to challenge the Investigatory Powers Act.

“When you have declared yourselves to be God – which is what the Investigatory Powers Act does – there are no powers left to take,” says Anderson.

## Book Review: ‘Virtual Terror’

Source: <https://intpolicydigest.org/2017/08/11/book-review-virtual-terror/>

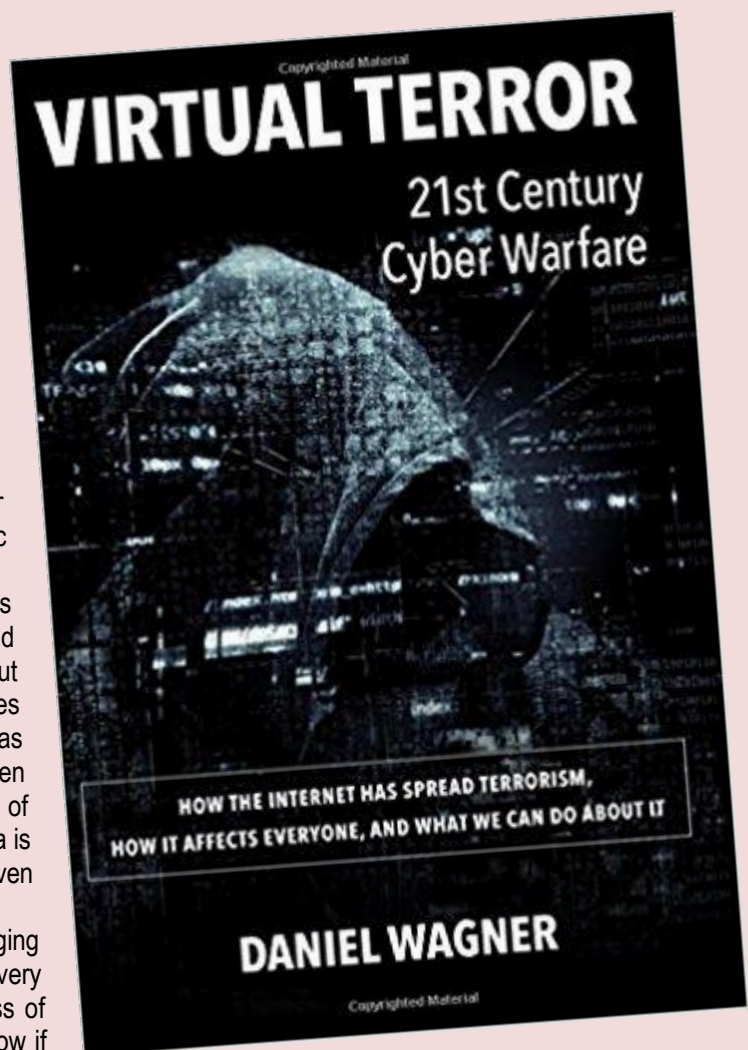
Aug 11 –“Terrorism” has needed to be redefined for quite some time now, as the cyber era has overtaken what terrorism ‘used’ to be. In his new book, [Virtual Terror](#), Daniel Wagner not only redefines what terrorism has become, but intricately dissects how it impacts each of us. He starts by redefining what cyber terrorism is: it does not matter who is the cyber terror perpetrator – whether an individual, group, business, or government – because if you happen to be on the receiving end of their actions, the net result is the same. Not only have terrorists’ methods changed, but the breadth and depth of the damage they cause has morphed as well, while our ability to effectively combat them is being consistently diminished.

It is this sense of powerlessness to do much about it that is a recurring theme in the book, which is breathtakingly broad in scope. Wagner ‘sets the table’ by putting *Virtual Terrorism* into context, highlighting some of the best-known examples of cyberterrorism and the implications of Internet-based threats. He then provides a cornucopia of lesser known examples that help to drive chapter-specific themes.

One of the best things about Wagner’s approach is that the reader is simultaneously entertained and terrified, making it, in a sense, less a book about terrorism per se than about the dangers and realities of living in an Internet-based world. That world has nooks and crannies most of us have never even contemplated, such as, the psychological impact of cyber theft and cyber bullying, and how social media is being used to penetrate lives that would never even otherwise be visible.

Most of us never even think about the dangers of logging on to the Internet or using our smartphones, but every time we do so, we are exposing ourselves to a loss of control not only of our privacy, but the ability to know if someone is watching us, what they want, when they plan to strike, or how they intend to harm us. Virtual terrorists operate in an invisible, anonymous, borderless, and lawless world where attribution is extremely difficult to identify, much less prove or prosecute.

From governments and the private sector to financial institutions and telecoms, and from bioterrorism and biometrics to drones and artificial intelligence, Wagner takes us on a rollercoaster ride into a world of astonishingly frightening possibilities in the future. All is not entirely dark, however, despite the book’s foreboding cover. The last part of the book focuses on how the law might



**CBRNE-TERRORISM NEWSLETTER – August 2017**

come to have more teeth, and what we can do to protect ourselves. The final chapter is a vision for what our near-term future may look like in this cyber-dominated world.

*Virtual Terror* is, in the end, a clarion call for what individuals, businesses, and governments need to do to try to combat this menace. Each has a comparative advantage and disadvantage, and Wagner calls for all sectors to find a way to work together more meaningfully. A siloed approach to combatting Virtual Terrorism simply will not work. He is right that, if we do not find a way to get out in front of this soon, the battle will likely be lost. This is a must read for anyone who understands that the best way to fight your enemy is to know it.







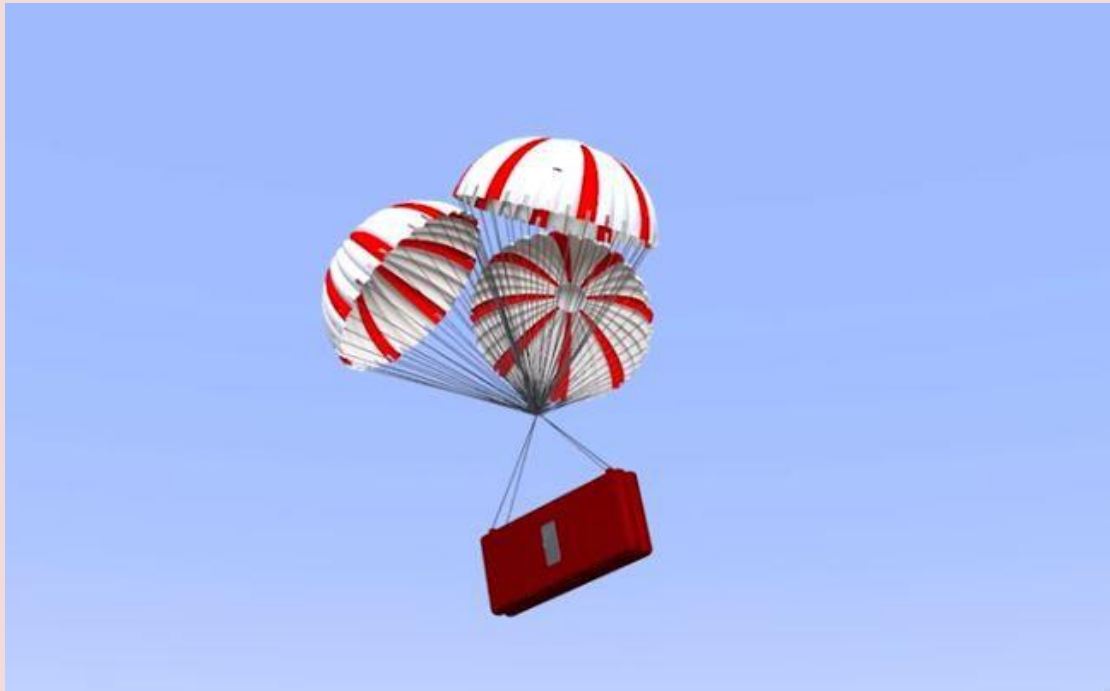
# EMERGENCY RESPONSE





## NestFold - NASA Space Apps Challenge 2017

Source: <https://www.youtube.com/watch?v=1VeRbg5ELLY>



First prize from NestFold Team (Cyprus).

## Better technologies help first responders respond more quickly, safely, and effectively

Source: <http://www.homelandsecuritynewswire.com/dr20170725-better-technologies-help-first-responders-respond-more-quickly-safely-and-effectively>



July 25 – When disaster strikes, first responders rush in to provide assistance. In addition to their courage and training, they depend on a panoply of technologies to do their jobs.

The Department of Energy's [Pacific Northwest National Laboratory](#) (PNNL) has partnered with emergency management and public safety professionals to define, develop, test and deploy these technologies to improve response and recovery. The Lab also applies its scientific capabilities to assess emergencies as they unfold.



**CBRNE-TERRORISM NEWSLETTER – August 2017**

Steven Ashby, director of Pacific Northwest National Lab, [writes](#) that PNNL manages the Department of Homeland Security's Responder Technology Alliance with the DHS Science and Technology Directorate (S&T), where the Lab's researchers work shoulder to shoulder with the responder community to evaluate how emerging technologies can help keep them safe and do their jobs better. For example, PNNL is developing wearable sensors and portable communications devices and helping put these solutions into action.

In one project, DHS, PNNL, and ADI Technologies developed a prototype wearable, hands-free communications system that enables multiple on-scene agencies and various incident command and control personnel to collaborate. Now available commercially, the wireless voice- and motion-operated device looks like a streamlined headset. It features a noise-filtering digital speaker and microphone, streaming video and translation capability — at a quarter of the cost of today's conventional radios.

PNNL researchers also are developing a collaboration space for the emergency management community and working with regional partners to evaluate its merits. This space allows users to share and store critical information such as video, voice, pictures, instant messages and documents on shared whiteboards and desktops in real time — and tailored to facilitate collaborative decision-making.

Ashby notes that another effort illustrates how PNNL bridges the gap between technology developers and first responders. A PNNL-developed electronic guide helps first responders make informed choices about the equipment and supplies available to rapidly collect, screen and identify biological threats in the field. The guide has been downloaded more than 14,000 times and is available as an app for iPhones and iPads. PNNL scientists also conducted more than 5,000 independent tests on 36 different technologies that enable responders to quickly screen suspicious powders that may contain anthrax or ricin.

PNNL has developed technology to assist in recovery following an incident, such as a biological or chemical contamination. The Lab's award-winning micro aerosol disinfecting system uses an electrochemically activated salt spray to kill bacteria, viruses and molds in enclosed spaces such as hospital rooms, vehicles and machinery. Not only is the system 99.9999 percent effective in killing a range of pathogens ranging from Staph to Ebola, it is easier to apply than other methods.

In addition to partnering on technology solutions, PNNL draws upon its science and engineering expertise to help respond to emergencies around the world. In 2011, after the earthquake and tsunami in Fukushima, Japan, PNNL provided early estimates of radiation releases and potential exposures, assisted with stabilizing the site of the nuclear reactors and putting the plant into safe mode, and is now helping develop clean-up plans.

PNNL experts were also consulted following the 2010 Deepwater Horizon disaster in the Gulf of Mexico, where they used modeling to estimate the amount of oil that was leaking. And this past spring, several of the Lab staff received a Secretary of Energy commendation for their efforts in the global response to the 2014 Ebola epidemic in Western Africa.

Finally, PNNL researchers are helping to improve preparedness and response for future disasters. For example, the Lab is applying its world-leading data analytics capabilities to support development of predictive flood analytics for DHS. In collaboration with the National Weather Service, PNNL developed a prototype tool to better forecast how high rivers will rise and pinpoint the extent of potential flooding.

"From technology development to deployment, PNNL is bringing innovation to first response and incident recovery. By partnering with those who protect us, we are helping to make them even more effective and keeping them safe," Ashby concludes.

### **Three advanced first-response technologies funded**

Source: <http://www.homelandsecuritynewswire.com/dr20170725-three-advanced-firstresponse-technologies-funded>

July 25 – During its meeting on 14 June 2017, held in Washington, D.C., the Board of Governors of the Israel-U.S. [Binational Industrial Research and Development](#) (BIRD) Foundation [awarded](#) funding to three homeland security projects, selected by DHS and MOPS, between U.S. and Israeli companies to advance technologies for first responders. In addition to the grants from BIRD, the projects will access private sector funding, boosting the total value of the three projects to approximately \$7 million.



**CBRNE-TERRORISM NEWSLETTER – August 2017**

The program funds technology collaborations between U.S. and Israeli partners that have significant commercial potential to meet the most pressing requirements of first responders. This joint research effort

supports the development of Next Generation First Responder (NGFR) technology capabilities that will increase the safety and efficiency of all first responders (law enforcement, firefighters and emergency medical services). These research and development efforts will lead to new technologies that ensure first responders are better protected, connected and fully aware.

The BIRD Foundation promotes collaboration between U.S. and Israeli companies in various technological fields for the purpose of joint product development. In addition to providing conditional grants of up to \$1 million for approved projects, the Foundation assists by working with companies to

identify potential strategic partners and facilitate introductions.

Projects submitted for consideration are reviewed by representatives of the U.S. Department of Homeland Security, the Israel Innovation Authority and experts from the Israel Ministry of Public Security.

**The joint projects that received approval include:**

— **Beeper Communications Israel** (Ramat Gan, Israel) and **Mantaro Networks Inc.** (Germantown, Maryland) will develop an unmanned search and rescue system.

— **Elbit Systems Land and C4I Ltd.** (Netanya, Israel) and **M87, Inc.** (Bellevue, Washington) will develop public safety off-network broadband communications using multi-hop WiFi/LTE/D2D communications (ProSE) technology.

— **Simlat, Ltd** (Petah-Tikva, Israel) and **Sinclair Community College** (Dayton, Ohio) will develop an autonomous drone-based search & rescue solution.

Acting Under Secretary William N. Bryan, for the U.S. Department of Homeland Security Science and Technology Directorate stated, "I am delighted to have this opportunity to work with the Israeli Ministry of Public Security and the BIRD Foundation to bring the best of U.S. and Israeli technology companies together to develop capabilities to support our first responders. First responders across the world share common needs and capabilities, and the benefits of these partnership activities will enhance first responders' safety and effectiveness across the globe."

Dr. Gad Frishman, Chief Scientist of the Israeli Ministry of Public Security said: "The Office of the Chief Scientist sees the cooperation with the BIRD Foundation as one of the main mechanisms to develop and commercialize innovative Israeli technologies which will enhance the emergency preparedness abilities of First Responders. The process of identifying the needs and selecting projects in cooperation with the U.S. Department of Homeland Security allows for mutual benefit and paves the way for success."

Dr. Eitan Yudilevich, Executive Director of the BIRD Foundation, said, "This second cycle of projects relating to first responder technologies reflects the potential of Israeli and American companies to jointly develop products and technologies that will keep tomorrow's first responders more protected, connected and fully aware. We look forward to continue working closely with DHS and MOPS to foster and facilitate partnerships that respond to the capability gaps that exist in this market."

**Extreme weather seen killing 152,000 Europeans a year by 2100**

Source: <http://www.euronews.com/2017/08/05/extreme-weather-seen-killing-152000-europeans-a-year-by-2100>

Aug 05 – Europe's death toll from weather disasters could rise 50-fold by the end of this century, with extreme heat alone killing more than 150,000 people a year by 2100 if nothing is done to curb the effects of climate change, scientists said on Friday. In a study in *The Lancet Planetary Health* journal, the scientists said their findings showed climate change placing a rapidly increasing burden on society, with two in three people in Europe likely to be affected if greenhouse gas emissions and extreme weather events are not controlled. The predictions, based on an assumption of no reduction in greenhouse gas emissions and no improvement in policies to reduce the impact of extreme climatic events, show European weather-related deaths rising from 3,000 a year between 1981 and 2010 to 152,000 a year between 2071 and 2100. "Climate change is one of the biggest global threats to human health of the 21st century, and its peril to society will be increasingly connected to





**CBRNE-TERRORISM NEWSLETTER – August 2017**

weather-driven hazards,” said Giovanni Forzieri of the European Commission Joint Research Centre in Italy, who co-led the study. He said that “unless global warming is curbed as a matter of urgency”, some 350 million Europeans could be exposed to harmful climate extremes on an annual basis by the end of the century.

The study analysed the effects of the seven most harmful types of weather-related disaster – heat waves, cold waves, wildfires, droughts, river and coastal floods and windstorms – in the 28 countries of the European Union, plus Switzerland, Norway and Iceland. The team looked at disaster records from 1981 to 2010 to estimate population vulnerability, then combined this with modelling of how climate change might progress and how populations might increase and migrate. Their findings suggested heat waves would be the most lethal weather-related disaster and could cause 99 percent of all future weather-related deaths in Europe – rising from 2,700 deaths a year between 1981 and 2010 to 151,500 deaths a year in 2071 to 2100. The results also predicted a substantial rise in deaths from coastal flooding, from six deaths a year at the start of the century to 233 a year by the end of it. The researchers said climate change would



be the main driver, accounting for 90 percent of the risk, while population growth, migration and urbanisation would account for 10 percent. Paul Wilkinson, a professor at the London School of Hygiene and Tropical Medicine who was not involved in the research, said its findings were worrying. “Global warming could result in rapidly rising human impacts unless adequate adaptation measures are taken, with an especially steep rise in the mortality risks of extreme heat,” he said. The findings add “further weight to the powerful argument for accelerating mitigation actions” to limit emissions, slow climate change and protect population health, Wilkinson said.



## **Gatlinburg Wildfire Records Tell Story of Chaos, Confusion**

Source: <http://www.govtech.com/em/disaster/Gatlinburg-Wildfire-Records-Tell-Story-of-Chaos-Confusion.html>



**CBRNE-TERRORISM NEWSLETTER – August 2017**

Aug 10 – Everything failed in an instant.

Severed lines snuffed out power to the command center directing the emergency response to the deadly Gatlinburg wildfires the night of Nov. 28 and plunged firefighting and rescue efforts into darkness and chaos.

Sevier County began releasing records Wednesday documenting the confusion caused by the collapse of communications systems as fire swept into the city.

Records released earlier by Pigeon Forge and Sevierville — from E-911 calls to radio traffic — also show how those agencies struggled frantically to protect their communities and help save Gatlinburg while blinded, hobbled and struck deaf by one critical system failure after another.



High winds and roaring flames about 8:30 p.m. disabled cell towers, melted fiber-optic cables, disrupted digital radio signals and shut down phone lines. Backup systems and protocols failed. With more than 1,000 radios on Sevier County's 10-channel Kenwood emergency radio system, police, fire and rescue messages choked the system with a flood of traffic.

Police officers, firefighters, rescue squad volunteers and dispatchers found themselves cut off from each other, trying to direct the battle against East Tennessee's worst fire of the 21st century with little more than Stone Age communication technology. Word of mouth was the only thing left in some cases.

Neighboring cities couldn't be sure where to send mutual aid. Authorities in Nashville couldn't get a handle on how to coordinate the statewide response.

Callers to Sevier County's E-911 Center so overloaded the system, their pleas for help ended up at the Putnam County E-911 Center in Cookeville, 150 miles away, said John Mathews, director of the Sevier County Emergency Management Agency.

Other calls rolled over to Sevierville Fire Department stations.

Mathews said the E-911 Center's telephone provider still can't explain how emergency calls were routed to Putnam County in Middle Tennessee. It's the first time in memory, he said, that E-911 calls somehow rolled over to Sevierville fire stations.

"We can't talk to Gatlinburg," a Pigeon Forge Police Department dispatcher complained about 11 p.m. "They've got nothing."

Even the state's top E-911 technology guru couldn't find a solution.

"Is Gatlinburg going to be able to evacuate?" Eddie Burchell, chief of technology for the Tennessee Emergency Communications Board, asked a Pigeon Forge dispatcher at 9:42 p.m.

The near-total blackout cost precious time in targeting first responders to the erupting fires, spread confusion among residents and visitors, and undermined efforts to send a mobile evacuation alert. Tennessee Emergency Management officials said sending a bare-bones evacuation notice via text message over the state Integrated Public Alert and Warning System, or IPAWS, with no concrete details from responders on the ground would have created a panic and done more harm than good.

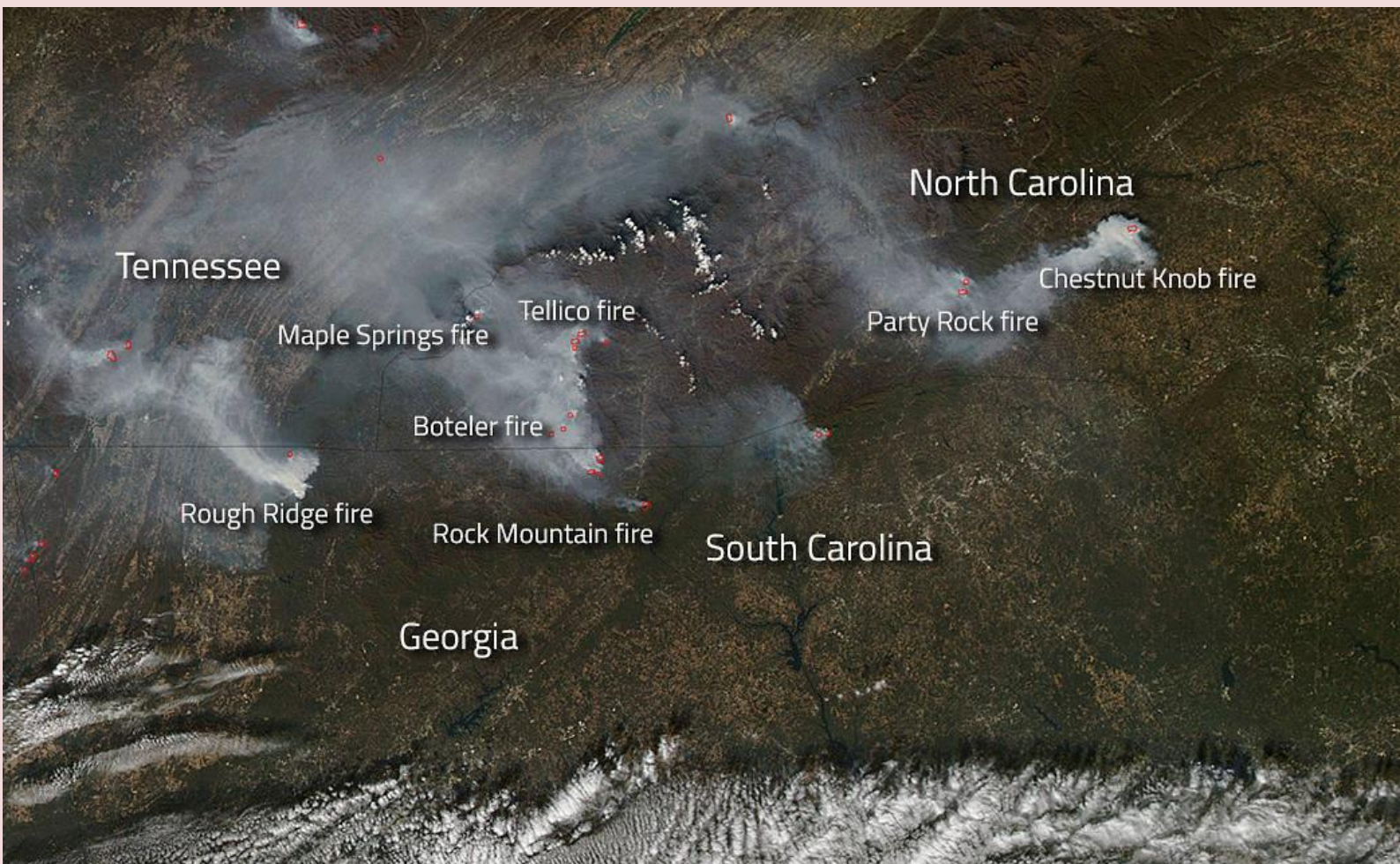




**CBRNE-TERRORISM NEWSLETTER – August 2017**

"So much was happening so fast," said Patrick Sheehan, TEMA director. "We were getting conflicting reports. Our liaison was on his way to the scene and stuck in traffic on (U.S.) Highway 321 (outside town). At some point, the news stations told us there was a mandatory evacuation. We tried to re-establish contact with Sevier County. Every redundant system we had in place for a period of time was not working." Sheehan said TEMA's channel on the \$120 million statewide Motorola radio system couldn't maintain a connection with the emergency team in Gatlinburg. Even ham radio systems weren't available, Sheehan said.

The fire had burned for nearly a week inside the Great Smoky Mountains National Park along the remote Chimney Tops Trail when winds that approached 90 mph sent the flames coursing through Gatlinburg and parts of Pigeon Forge and Sevier County around 6 p.m. on Nov. 28. Burning debris and toppled power lines started at least 20 fires in the space of a quarter-hour, officials said, and raged throughout the night into the next day. Fourteen people died, nearly 200 suffered various injuries, and nearly 2,500 homes and businesses were damaged or destroyed. Authorities have placed the final recovery estimate



at roughly \$1 billion.

TEMA officials didn't know the downed power lines had shut down Gatlinburg's emergency operations center and dispatch system. The city's dispatchers relied at the time on an internet-based phone system with no backup in place, Police Chief Randy Brackins said.

"When the computers are off, the system's off," he said. "It was down at least a couple of days. The radio service was so busy, we had to try to communicate by cellphone."

Sevier County's central dispatch operates out of the E-911 center in Sevierville. That's where the first calls came in about fires erupting throughout Gatlinburg. Either from downed electrical lines or embers described "as large as a football" from the National Park wildfire, the fires were spreading.

Normally, Mathews said, the E-911 center determines the emergency and sends the call along. If it's a police matter in Pigeon Forge, Sevierville or Gatlinburg, the call would be





**CBRNE-TERRORISM NEWSLETTER – August 2017**

switched to that agency's radio dispatcher. All fire and medical calls remain in the E-911 center and become the responsibility of central dispatch. Mathews said four or five dispatchers handle those calls, sending fire engines from Gatlinburg, Sevierville, Pigeon Forge or a volunteer agency to reported fires.

Once firefighters arrive at a scene, fire commanders take charge of the personnel and radio communications.

Clogged airwaves and crippled cell towers made for hit-or-miss coverage. High winds disrupted the digital network relied on by TEMA's statewide radio system, Sheehan said.

Sheehan finally reached Mathews by cell and offered to send an evacuation alert to every cellphone in the area — but not without Mathews' direction and approval.

"We can't just say, 'Evacuate.' That would be irresponsible," Sheehan said. "We don't know whether there are trees or power lines across which roads."

Sheehan and TEMA spokesman Dean Flener drafted an alert, recommending Highway 321 as an evacuation route and directing anyone in Gatlinburg to one of the emergency shelters set up nearby. That alert never went out.

TEMA and Sevier County had lost contact again. Without Mathews' approval, no message would be sent. "At this point, I have an unverified message," Flener said. "I need to make sure the message is accurate. We didn't have the information to send (an alert) that was accurate, so we didn't."

The only text alert from TEMA that reached anyone was a notice sent hours after the fire began, asking residents to stay off their cellphones. Flener said that request helped and seemed to open cellphone access for emergency personnel.

On the ground in Sevier County, word of the evacuation spread slowly. Officials about 8 p.m. activated downtown Gatlinburg's siren warning system and broadcast news of the evacuation on TV and radio, but not everyone got the message. Calls jammed dispatch centers outside Gatlinburg as residents and tourists tried to find out whether they should flee the approaching blaze.

"I'd stay vigilant throughout the night," a Sevierville dispatcher told one caller.

Fire crews couldn't reach utility companies to shut off power grids. Pigeon Forge at one point resorted to dispatching officers by text message to assist with evacuating homes and campgrounds.

**Pigeon Forge firefighters relied on the Kenwood radio system. Pigeon Forge police used a Motorola 700 megahertz radio system. Neither system fared well.**

Some officers wound up calling their dispatchers with cellphones to find out where other officers were. Some residents didn't want to leave. One man called Pigeon Forge dispatchers to insist he could fight off the flames with his garden hose. A woman asked what would happen if she ignored the evacuation order. "You need to leave," came the reply.





ICI  
International  
**CBRNE**  
INSTITUTE



# ASYMMETRIC THREATS



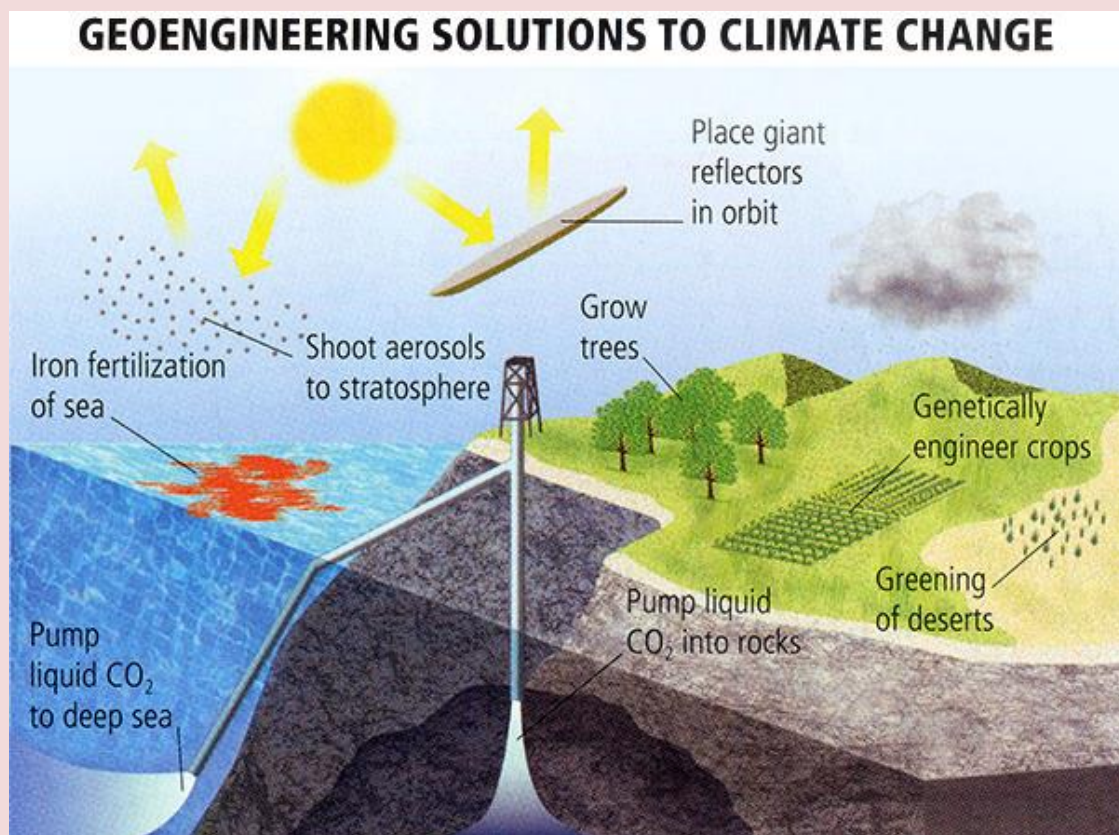


## A “cocktail” of geoengineering approaches to combat climate change

Source: <http://www.homelandsecuritynewswire.com/dr20170725-a-cocktail-of-geoengineering-approaches-to-combat-climate-change>

July 25 – Geoengineering is a catch-all term that refers to various theoretical ideas for altering Earth's energy balance to combat climate change. New research from an international team of atmospheric scientists published by *Geophysical Research Letters* investigates for the first time the possibility of using a “cocktail” of geoengineering tools to reduce changes in both temperature and precipitation caused by atmospheric greenhouse gases.

Carbon dioxide emissions from the burning of coal, oil, and gas not only cause the Earth to get hotter, they also affect weather patterns around the world. Management approaches need to address both warming and changes in the amount of rainfall and other forms of precipitation.



So-called solar geoengineering aims to cool the planet by deflecting some of the Sun's incoming rays. Ideas for accomplishing this include the dispersion of light-scattering particles in the upper atmosphere, which would mimic the cooling effect of major volcanic eruptions.

Carnegie Institution for Science [notes](#), however, that climate-modeling studies have shown that while this scattering of sunlight should reduce the warming caused by greenhouse gases in the atmosphere, it would tend to reduce rainfall and other types of precipitation less than would be optimal.

Another approach involves thinning of high cirrus clouds, which are involved in regulating the amount of heat that escapes from the planet to outer space. This would also reduce warming, but would not correct the increase in precipitation caused by global warming.

One method reduces rain too much. Another method reduces rain too little.

This is where the theoretical cocktail shaker gets deployed.

The team—which includes Carnegie's Ken Caldeira, Long Cao and Lei Duan of Zhejiang University, and Govindasamy Bala of the Indian Institute of Science—used models to simulate what would happen if sunlight were scattered by particles at the same time as the





**CBRNE-TERRORISM NEWSLETTER – August 2017**

cirrus clouds were thinned. They wanted to understand how effective this combined set of tools would be at reversing climate change, both globally and regionally.

“As far as I know, this is the first study to try to model using two different geoengineering approaches simultaneously to try to improve the overall fit of the technology,” Caldeira explained.

The good news is that their simulations showed that if both methods are deployed in concert, it would decrease warming to pre-industrial levels, as desired, and on a global level rainfall would also stay at pre-industrial levels. But the bad news is that while global average climate was largely restored, substantial differences remained locally, with some areas getting much wetter and other areas getting much drier.

“The same amount of rain fell around the globe in our models, but it fell in different places, which could create a big mismatch between what our economic infrastructure expects and what it will get,” Caldeira added. “More complicated geoengineering solutions would likely do a bit better, but the best solution is simply to stop adding greenhouse gases to the atmosphere.”

Caldeira said that the international collaboration of scientists (including scientists from China and India) undertook this research as part of a broader effort aimed at understanding the effectiveness and unintended consequences of proposed strategies for reducing climate change and its impacts.

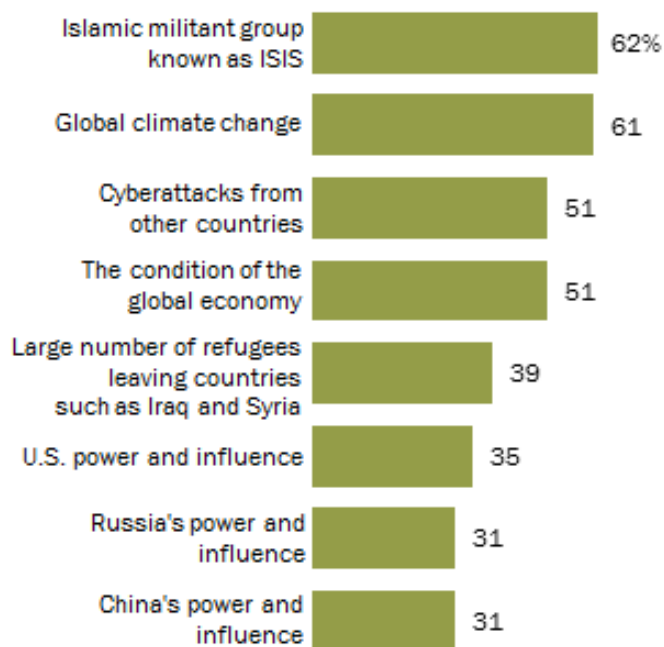
— Read more in Long Cao et al., “Simultaneous stabilization of global temperature and precipitation through cocktail geoengineering,” [Geophysical Research Letters](#) (24 July 2017).

## ISIS and climate change leading security threats: Global survey

Source: <http://www.homelandsecuritynewswire.com/dr20170801-isis-and-climate-change-leading-security-threats-global-survey>

### ISIS and climate change seen as among top threats around the world

\_\_\_ is a major threat to our country



Note: Figures represent global medians across 38 countries. ISIS not asked in Turkey, U.S. power and influence not asked in U.S., and Russia's power and influence not asked in Russia.

Source: Spring 2017 Global Attitudes Survey. Q17a-h.

PEW RESEARCH CENTER

Aug 01 – People around the globe identify ISIS and climate change as the leading threats to national security, according to a new Pew Research Center [report](#) based on a survey of thirty-eight countries.

The survey asked about eight possible threats: ISIS, global climate change, cyberattacks, the condition of the global economy, the large number of refugees leaving Iraq and Syria, and the power and influence of the United States, Russia, and China. While the level and focus of concern varies by region and country, ISIS and climate change clearly emerge as the most frequently cited security risks across the thirty-eight countries polled.

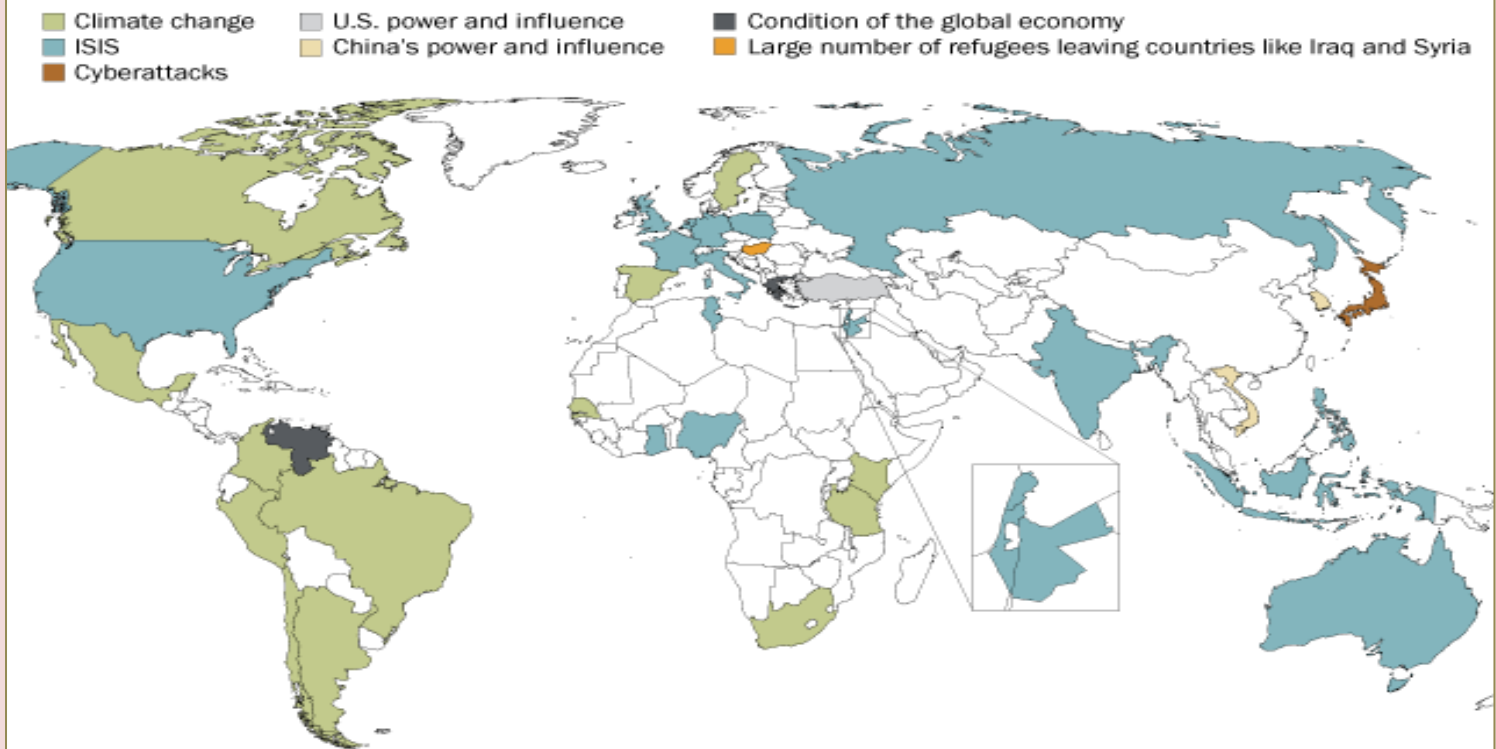
ISIS is named as the top threat in a total of eighteen countries surveyed – including the United States and others mostly concentrated in Europe, the Middle East, and Asia. A substantial number of these countries have endured deadly terrorist attacks claimed by the Islamic militant group. In thirteen countries, mostly in Latin America and Africa, publics identify global climate change as the topmost threat. It is the second-ranked concern in many other countries polled.

Cyberattacks from other countries and the condition of the global economy are named as major threats by global medians of 51 percent each. Cyberattacks are the top concern in Japan and second-highest concern in places such as the United



## Greatest threats around the world

*Top threat to (survey country)*



Note: U.S. power and influence not asked in the U.S., Russia's power and influence not asked in Russia, ISIS not asked in Turkey.  
Source: Spring 2017 Global Attitudes Survey. Q17a-h.

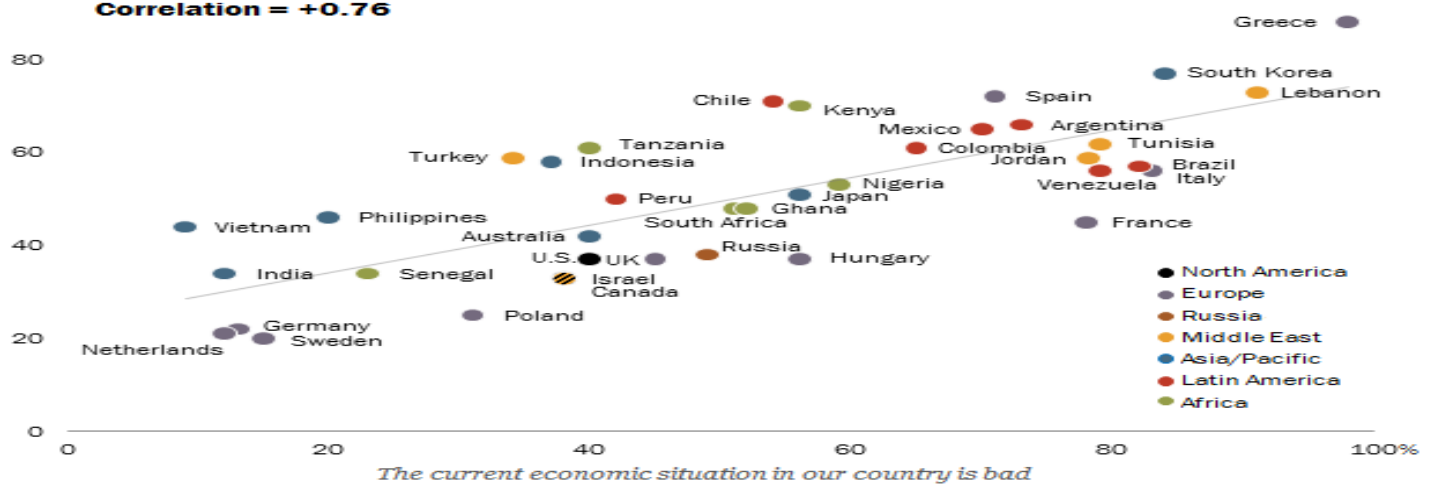
States, Germany, and the United Kingdom, where there have been a number of high-profile attacks of this type in recent months.

## Publics that see their countries struggling economically tend to feel more threatened by the condition of the global economy

*The condition of the global economy is a major threat to our country*

100%

**Correlation = +0.76**



Source: Spring 2017 Global Attitudes Survey. Q17h.

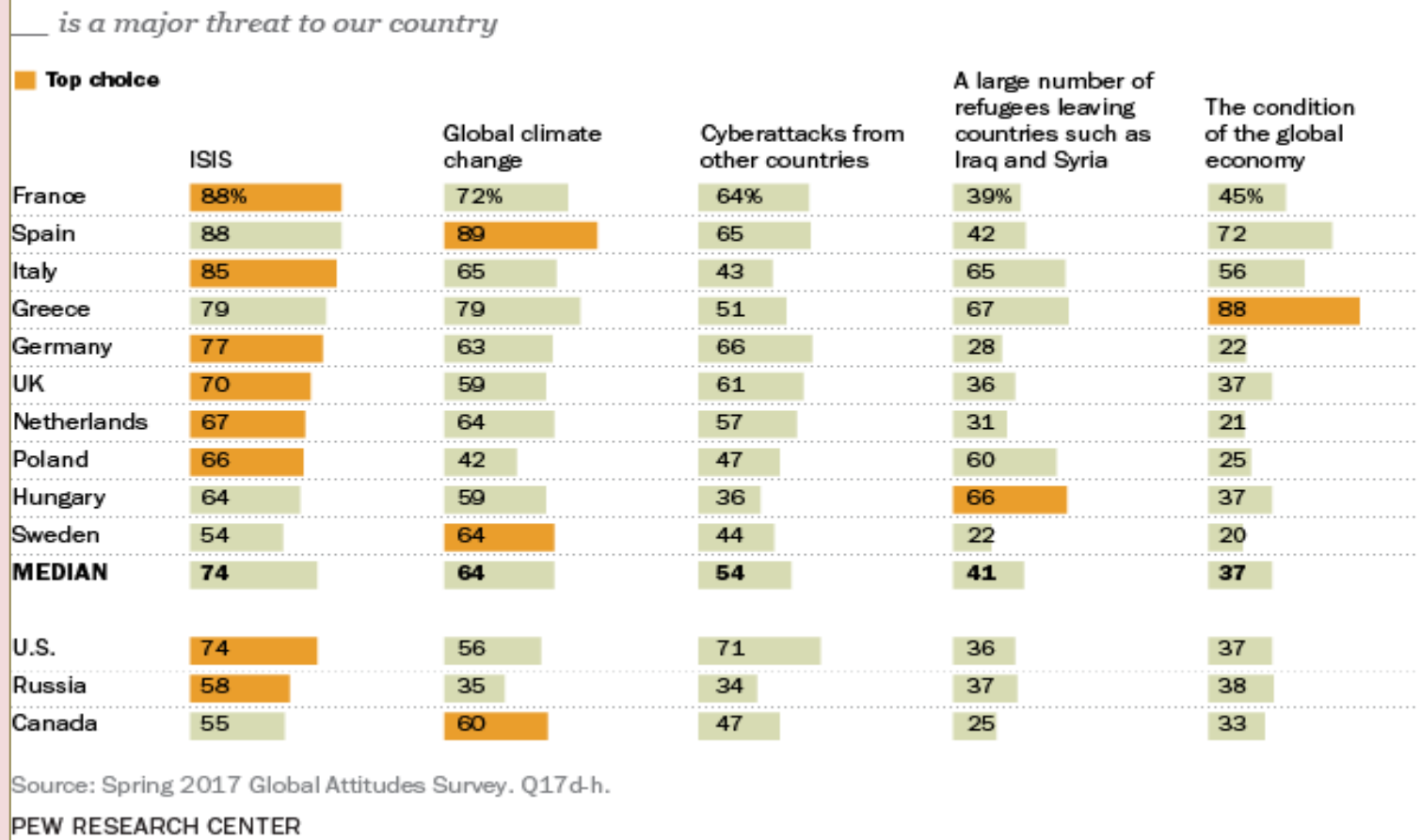
PEW RESEARCH CENTER

People in Greece and Venezuela view the health of the international economy as the leading threat to their countries, perhaps reflecting these nations' economic struggles in recent years. Many countries surveyed in the Middle East and Latin America name economic



**CBRNE-TERRORISM NEWSLETTER – August 2017**

turmoil as their second-greatest concern. The influx of refugees, which was of particular concern in Europe in 2016, is seen as a major threat by a median of 39 percent across the thirty-eight countries. It

**Across much of Europe, ISIS is top concern**

is the top threat in only one country, however: Hungary.

Globally, a median of about one-third view the power and influence of the United States, Russia, or China as a major threat. America's influence is a top concern in Turkey. And in South Korea and Vietnam, eight-in-ten or more name China's power and influence as a major threat. Meanwhile, among the countries surveyed, fears of Russia are most acute in Poland.

These are among the major findings of a Pew Research Center survey conducted among 41,953 respondents in thirty-eight countries from 16 February to 8 May 2017.

►► The findings are available [here](#).

## **Germans are more afraid of climate change than terrorism or mass immigration – poll**

Source: <https://www.rt.com/news/398380-germans-climate-change-poll/>

Aug 02 – **Most Germans consider climate change a much greater cause for concern than such headline-grabbing issues as terrorism or the refugee crisis, a recent poll has showed.**

Climate change surprisingly emerged as Germany's greatest fear as 71 percent of respondents designated it as a particular source of serious personal concern, the poll conducted by the Kantar Emnid opinion research center on commission from the German Funke Media Group revealed.





**CBRNE-TERRORISM NEWSLETTER – August 2017**

The future state of the environment left behind such pressing issues as the threat of terrorist attacks or the possibility of new wars, which were identified as reasons for unease by 63 and 65 percent of respondents respectively.

The massive immigration and subsequent refugee crisis that repeatedly hit the headlines in the German and international media turned out to be even further behind (45%) on the list of the Germans' anxieties, surpassed by old-age poverty.

Potential unemployment turned out to be the least worrisome problem for Germans, as only about one third of respondents said it gave them cause for concern. Slightly more than 60 percent of those polled said they were concerned with the present crime rate in Germany. Supporters of the populist anti-immigrant Alternative for Germany (AfD) party were the only ones who described the immigration and refugee crisis as their primary concern as 90 percent of them called it their biggest fear, the survey found. The backers of the Left Party seemed to be less concerned about the environment and more about potential poverty in old age.

## Greatest Security Threat: Climate Change or ISIS?



**CLARION**  
project

*"Environment and climate protection have already greatly mattered to people in Germany for years,"* Torsten Schneider-Haase, head of the political research department at Kantar Emnid center told the Funke Media Group, commenting on the survey results.

He added that *"the fight against climate change has been understood as a cross-party effort,"* explaining why supporters of most major German parties described it as their primary concern as well as why support for the German Green Party, which made climate change its main political agenda, remains relatively low. He also said that *"security-related topics still play a significant role,"* adding that issues related to *"the external, internal and social security"* still occupy the minds of the Germans. *"A party such as [the German Chancellor Angela Merkel's Christian Democratic] Union (CDU), which is considered to be competent in the security issues, is in a good position ahead of the forthcoming elections,"* he concluded.

The poll results come at a time when Germany faces an increased security threat posed by various extremist groups.

The country endured several high-profile terrorist attacks last year. The most notable of these happened in December, when a Tunisian asylum seeker, who pledged allegiance to Islamic State, plowed a truck into a Berlin Christmas market, killing 12 people. Before that, in July, a Syrian refugee detonated an explosive device outside a music festival in the town of Ansbach, killing himself and injuring 12 others. In another July 2016 incident, an Afghan teen attacked train passengers in central Germany, leaving five people injured.

Islamic State (IS, former ISIS/ISIL) claimed responsibility for all the attacks.

German media has repeatedly reported about terrorist suspects plotting attacks on German territory over the course of the year. In early July 2017, Hans-Georg Maassen, the head of the German domestic intelligence service, the BfV, warned the country is likely to see more terrorist attacks carried out by Islamist jihadists.

His remarks came as he presented the annual report on threats to the state, which said that some 24,400 Islamists remain in Germany. The number included around 10,000 Salafists – an ultra-conservative movement within Sunni Islam, followers of which have been prone to terrorism.

However, it appears that Islamist extremism is not the only threat to Germany's security. Another government report released by the German interior ministry in June, says that more than 460 far-right extremists with arrest warrants are still at large in Germany. Ulla Jelpke, a lawmaker for Die Linke (The Left) party, said the figure indicates the presence of an "established Nazi underground."



**CBRNE-TERRORISM NEWSLETTER – August 2017**

Left-wing extremism also hit the headlines in Germany, particularly after the G20 summit in Hamburg which saw violent clashes between left-wing radicals and police. The violence left almost 500 security officials, including 180 federal police officers, injured, according to the German Interior Minister Thomas de Maiziere.

Following the G20 riots, German politicians demanded a radical change of approach toward violent protests as well as to left-wing extremism.

Meanwhile, a recent poll conducted by YouGov and Statista found that some 81 percent of Germans believe their country has a growing problem with political extremism – both far left and far right – with 78 percent of respondents saying the German government has lost control of dealing with the problem.

## Climate change shifts timing of floods in Europe

Source: <http://www.homelandsecuritynewswire.com/dr20170821-climate-change-shifts-timing-of-floods-in-europe>



An aerial view shows the flooded city centre of Grimma, eastern Germany, on June 3, 2013.

Aug 21 – A study conducted by TU Wien and thirty European partners shows that the timing of the floods has shifted across much of Europe, dramatically in some areas. When a major flood event occurs, it is often attributed to climate change. However, a single event is not proof, and so far, it has been unclear whether climate change has a direct influence on river floods at large scales in Europe.

A large international project led by Prof. Günter Blöschl from the Institute of Hydraulic Engineering and TUWien [says](#) Water Resources Management at TU Wien has now collected and analyzed fifty years of data from over 4,000 hydrometric stations from thirty-eight European countries. This is an unprecedented dataset in terms of coverage across Europe and

the sheer number and diversity of river systems that have been included.

The result: Climate change has a real impact on flood events in some regions. This has been seen by a shift in the timing of floods over the years. Depending on the cause of the flood events, they occur earlier in some regions, in others they occur later. The results have now been published in [Science](#).

### The magnitude does not tell you everything

"In flood research, we are often concerned with the annual probability of the occurrence of floods," says Blöschl. "By observing their magnitudes one can estimate a one hundred-year flood as a high-water event that occurs with a



probability of one percent in any one year.”

However, while probabilities and magnitudes are an essential aspect of flood risk management, they are not necessarily the most sensitive characteristics for detecting the impact of climate change, as they do not only depend on the climate: “If one only examines the magnitude of flood events, the role of the climate can be masked by other effects,” explains Blöschl. “Land use change by urbanization, intensifying agriculture and deforestations are other factors affecting flood events.”

#### **The timing provides information on the influence of the climate**

In order to understand the connection between climate and floods, Blöschl and his team looked closely at the timing of the flood events in different regions of Europe. “The timing of a flood provides information about its likely cause,” says Blöschl. For example, in much of north-west Europe and the Mediterranean, floods occur more frequently in the winter, when evaporation is low and precipitation is intense. In Austria, on the other hand, the highest magnitude floods are associated with summer downpours. In North-Eastern Europe, the risk of flooding is at its highest in spring because of snow melt. The timing at which floods occur is thus much more directly related to the climate, in contrast with the absolute magnitude of the flood event.

Flood data from all over Europe have been meticulously compiled, screened and statistically analysed. These show that the floods in Europe have indeed shifted considerably over the last fifty years: “In the north-east of Europe, Sweden, Finland and the Baltic States, floods now tend to occur one month earlier than in the 1960s and 1970s. At that time, they typically occurred in April, today in March,” says Blöschl. “This is because the snow melts earlier in the year than before, as a result of a warming climate.”

In parts of northern Britain, western Ireland, coastal Scandinavia and northern Germany, on the other hand, floods now tend to occur about two weeks later than they did a couple of decades ago. Later winter storms are likely to be associated with a modified air pressure gradient between the equator and the pole, which may also reflect climate warming. The study sheds light on the complexity of flood processes in north-western Europe; on the Atlantic coasts of Western Europe, ‘winter’ floods in fact typically occur earlier, in the autumn, as maximum soil moisture levels are now reached earlier in the year. In parts of the Mediterranean coast, flood events occurring later in the season are aligned with the warming of the Mediterranean.

“The timing of the floods throughout Europe over many years gives us a very sensitive tool for deciphering the causes of floods,” says Blöschl. “We are thus able to identify connections that previously were purely speculative.”

— Read more in Günter Blöschl et al., “Changing climate shifts timing of European floods,” [\*Science\* 357, no. 6351 \(11 August 2017\): 588-90.](#)







# BUSINESS CONTINUITY



Business Interruption

Disaster Event

## 2017 Risk Value Report: Business Security- Always a Journey, Never a Destination

Source: <https://www.infosecurity-magazine.com/white-papers/2017-risk-value-report>

This year's NTT Security Risk:Value Report comes at a critical point for businesses. The General Data Protection Regulation (GDPR) will come into force on 25 May 2018, leaving companies with less than a year to comply with strict new regulations around data privacy and security.

Register to download the report and learn how:

- Globally, only 40% of organisations, on average, believe that they will be subject to GDPR
- In the UK, just 39% of organisations currently identify GDPR as a compliance issue
- Outside Europe, many organisations are failing to see how the regulations will affect them, with only 25% of people in the US and 29% of people in Hong Kong understanding that their organisation will be subject to GDPR
- 33% of respondents don't know where their data is physically stored

Of those that do know, only 45% are 'definitely aware' of how GDPR will affect their data storage.

