Dedicated to Global First Responders

CBRNE NEWSLETTERRORISM

January 2017

www.cbne-terrorism-newsletter.com

Lost Nukes Present Opportunities for Terrorists

Source: http://i-hls.com/2017/01/lost-nukes-present-opportunities-terrorists/

Jan 01 – Could Islamist terrorists get a hold of a nuclear bomb? Dozens of nuclear warheads have gone missing during the 1950s, 60s, 70s and 80s – with many confirmed the loss of at least eight atomic bombs – with a combined explosive force 2,200 times the Hiroshima bomb.

According to The Sun, the Russians have never disclosed their missing weapons. However, according to the Berlin Information Centre for Transatlantic Security up to 50 nukes have been lost across the world since the 1950s. Most of these highly dangerous weapons are still lying on the ocean floor after military planes and subs sank without a trace.

Experts claim that while they would probably be no use as weapons they could easily be salvaged, and the uranium would be used to build a “dirty” bomb (a weapon that combines radioactive material with conventional explosives). ISIS terror fanatics, who have been working to bolster their ranks with a team of jihadi scientists capable of creating a dirty bomb, have already launched chemical attacks.

According to security service officials, finding a missing nuke would be a huge achievement for any terror group. Now, experts say the jihadis who want to develop nuclear weapons are the biggest threat to Europe since the end of the cold war.

Moshe Kantor, head of the Luxembourg Forum on Preventing Nuclear Catastrophe, warned: “ISIS has already carried out numerous chemical weapons attacks in Syria. We know it wants to go further by carrying out a nuclear attack in the heart of Europe”.

US president, Barack Obama, has warned the prospect of ISIS or other terrorists getting hold of a nuclear bomb is among the most serious threats faced by the world. Speaking during the international Nuclear Security Summit in Washington DC, earlier this year, he said it was clear that “these mad men” would use such a device to kill as many people as they could. Obama said the risk of ISIS or other extremists getting a nuclear weapon remains “one of the greatest threats to global security”, adding that ISIS had already used chemical weapons and that al-Qaeda had long sought nuclear material.

Frustration over the slow pace of reducing nuclear stockpiles shadowed this year’s summit, Obama’s final effort towards denuclearisation. The absence of key players further underscored the lack of unanimity still confronting global efforts to deter nuclear attacks.

8 Nuclear Weapons the U.S. Has Lost

Source: http://mentalfloss.com/article/17483/8-nuclear-weapons-us-has-lost

During the Cold War, the United States military misplaced at least eight nuclear weapons permanently. These are the stories of what the Department of Defense calls "broken arrows"—America's stray nukes, with a combined explosive force 2,200 times the Hiroshima bomb.

STRAY #1: Into the Pacific

February 13, 1950. An American B-36 bomber en route from Alaska to Texas during a training exercise lost power in three engines and began losing altitude. To lighten the aircraft the crew jettisoned its cargo, a 30-kiloton Mark 4 (Fat Man) nuclear bomb, into the Pacific Ocean. The conventional explosives detonated on impact, producing a flash and a shockwave. The bomb's uranium components were lost and never recovered. According to the USAF, the plutonium core wasn't present.

STRAY #2 & 3: Into Thin Air

March 10, 1956. A B-47 carrying two nuclear weapon cores from MacDill Air Force Base in Florida to an overseas airbase disappeared during a scheduled air-to-air refueling over the Mediterranean Sea. After becoming lost in a thick cloud bank at 14,500 feet, the plane was never heard from again and its wreckage, including the nuclear cores, was never found. Although the weapon type remains undisclosed, Mark 15 thermonuclear bombs (commonly carried by B-47s) would have had a combined yield of 3.4 megatons.

STRAYS #4 & 5: Somewhere in a North Carolina Swamp

January 24, 1961. A B-52 carrying two 24-megaton nuclear bombs crashed while taking off from an airbase in Goldsboro, North Carolina. One of the weapons sank in swampy farmland, and its uranium core was never found despite intensive search efforts to a depth of 50 feet. To ensure no one else could recover the weapon, the USAF bought a permanent easement requiring government permission to dig on the land.

STRAY #6: The Incident in Japan

December 5, 1965. An A-4E Skyhawk attack aircraft carrying a 1-megaton thermonuclear weapon (hydrogen bomb) rolled off the deck of the U.S.S. Ticonderoga and fell into the Pacific Ocean. The plane and weapon sank in 16,000 feet of water and were never found. 15 years later the U.S. Navy finally admitted that the accident had taken place, claiming it happened 500 miles from land the in relative safety of the high seas. This turned out to be not true; it actually happened about 80 miles off Japan's Ryuku island chain, as the aircraft carrier was sailing to Yokosuka, Japan after a bombing mission over Vietnam.

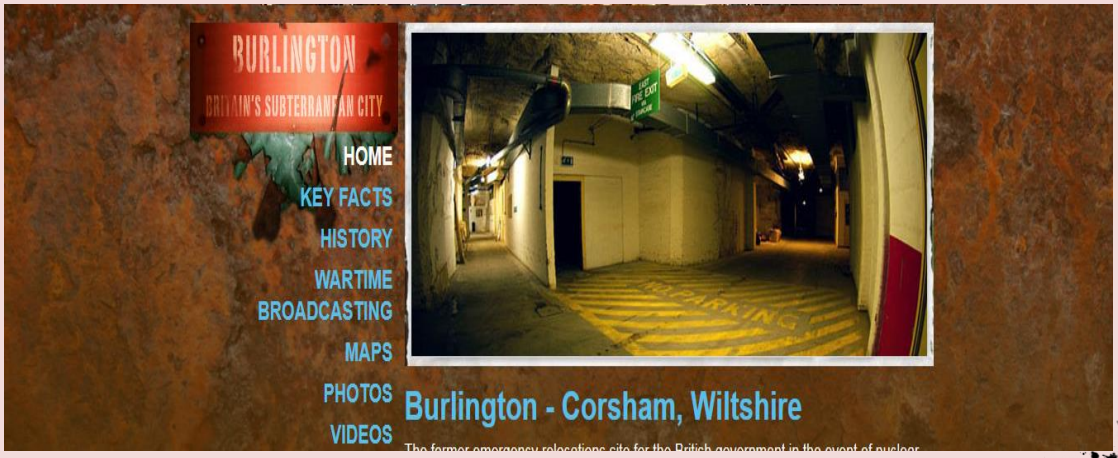
These revelations caused a political uproar in Japan, which prohibits the United States from bringing nuclear weapons into its territory.

STRAYS #7 & 8: 250 kilotons of explosive power

Spring, 1968. While returning to home base in Norfolk, Virginia, the U.S.S. Scorpion, a nuclear attack submarine, mysteriously sank about 400 miles to the southwest of the Azores islands. In addition to the tragic loss of all 99 crewmembers, the Scorpion was carrying two unspecified nuclear weapons—either anti-submarine missiles or torpedoes that were tipped with nuclear warheads. These could yield up to 250 kilotons explosive power (depending which kind of weapon was used).

NOTE: WHAT ABOUT TYBEE?

The United States lost a warhead off of Tybee Island, Georgia, in 1958. According to the U.S. Air Force, it did not contain a plutonium core and therefore could not be considered a functional nuclear weapon, though that has been debated. Whether you believe the U.S. Air Force on this matter is a personal call.



Source: http://www.burlingtonbunker.co.uk/

World War Three, by Mistake

By Eric Schlosser

Source: http://www.newyorker.com/news/news-desk/world-war-three-by-mistake

Dec 23, 2016 – On June 3, 1980, at about two-thirty in the morning, computers at the National Military Command Center, beneath the Pentagon, at the headquarters of the North American Air Defense Command (NORAD), deep within Cheyenne Mountain, Colorado, and at Site R, the Pentagon's alternate command post center hidden inside Raven Rock Mountain, Pennsylvania, issued an urgent warning: the Soviet Union had just launched a nuclear attack on the United States. The Soviets had recently invaded Afghanistan, and the animosity between the two superpowers was greater than at any other time since the Cuban Missile Crisis.

The NORAD headquarters, in Colorado Springs. PHOTOGRAPH BY PAUL CHELSEY / GETTY

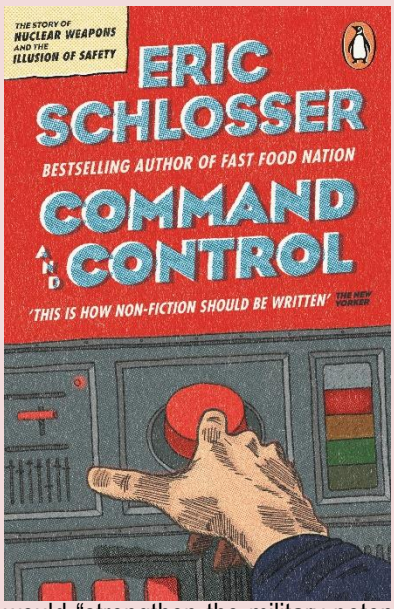
U.S. Air Force ballistic-missile crews removed their launch keys from the safes, bomber crews ran to their planes, fighter planes took off to search the skies, and the Federal Aviation Administration prepared to order every airborne commercial airliner to land.

President Jimmy Carter's national-security adviser, Zbigniew Brzezinski, was asleep in Washington, D.C., when the phone rang. His military aide, General William Odom, was calling to inform him that two hundred and twenty missiles launched from Soviet submarines were heading toward the United States. Brzezinski told Odom to get confirmation of the attack. A retaliatory strike would have to be ordered quickly; Washington might be destroyed within minutes. Odom called back and offered a correction: twenty-two hundred Soviet missiles had been launched.

Brzezinski decided not to wake up his wife, preferring that she die in her sleep. As he prepared to call Carter and recommend an American counterattack, the phone rang for a third time. Odom apologized—it was a false alarm. An investigation later found that a defective computer chip in a communications device at NORAD headquarters had generated the erroneous warning. The chip cost forty-six cents.

A similar false alarm had occurred the previous year, when someone mistakenly inserted a training tape, featuring a highly realistic simulation of an all-out Soviet attack, into one of NORAD's computers. During the Cold War, false alarms were also triggered by the moon rising over Norway, the launch of a weather rocket from Norway, a solar storm, sunlight reflecting off high-altitude clouds, and a faulty A.T. & T. telephone switch in Black Forest, Colorado.

My book **"Command and Control"** explores how the systems devised to govern the use of nuclear weapons, like all complex technological systems, are inherently flawed. They are designed, built, installed, maintained, and operated by human beings. But the failure of a nuclear command-and-control system can have consequences far more serious than the crash of an online dating site from too much traffic or flight delays caused by a software glitch. Millions of people, perhaps hundreds of millions, could be annihilated inadvertently. "Command and Control" focusses on near-catastrophic errors and accidents in the arms race between the United States and the Soviet Union that ended in 1991. The danger never went away. Today, the odds of a nuclear war being started by mistake are low—and yet the risk is growing, as the United States and Russia drift toward a new cold war. The other day, Senator John McCain called Vladimir Putin, the President of the Russian Federation, "a thug, a bully, and a murderer," adding that anyone who "describes him as anything else is lying." Other members of Congress have attacked Putin for trying to influence the Presidential election. On Thursday, Putin warned that Russia would "strengthen the military potential of strategic nuclear forces," and President-elect Donald Trump has responded with a vow to expand America's nuclear arsenal. "Let it be an arms race," Trump told one of the co-hosts of MSNBC's "Morning Joe." "We will outmatch them at every pass and outlast them all."



The harsh rhetoric on both sides increases the danger of miscalculations and mistakes, as do other factors. Close encounters between the military aircraft of the United States and Russia have become routine, creating the potential for an unintended conflict. Many of the nuclear-weapon systems on both sides are aging and obsolete. The personnel who operate those systems often suffer from poor morale and poor training. None of their senior officers has firsthand experience making decisions during an actual nuclear crisis. And today's command-and-control systems must contend with threats that barely existed during the Cold War: malware, spyware, worms, bugs, viruses, corrupted firmware, logic bombs, Trojan horses, and all the other modern tools of cyber warfare. The greatest danger is posed not by any technological innovation but by a dilemma that has haunted nuclear strategy since the first detonation of an atomic bomb: How do you prevent a nuclear attack while preserving the ability to launch one?

"The pattern of the use of atomic weapons was set at Hiroshima," J. Robert Oppenheimer, the scientific director of the Manhattan Project, said in November, 1945, just a few months after the Japanese city's destruction. "They are weapons of aggression, of surprise, and of terror." Nuclear weapons made annihilation vastly more efficient. A single bomb could now destroy a target whose elimination had once required thousands of bombs. During an aerial attack, you could shoot down ninety-nine per cent of the enemy's bombers—and the plane that you missed could obliterate an entire city. A war between two countries with nuclear weapons, like a Wild West shoot-out, might be won by whoever fired first. And a surprise attack might provide the only hope of national survival—especially for the country with an inferior nuclear arsenal.

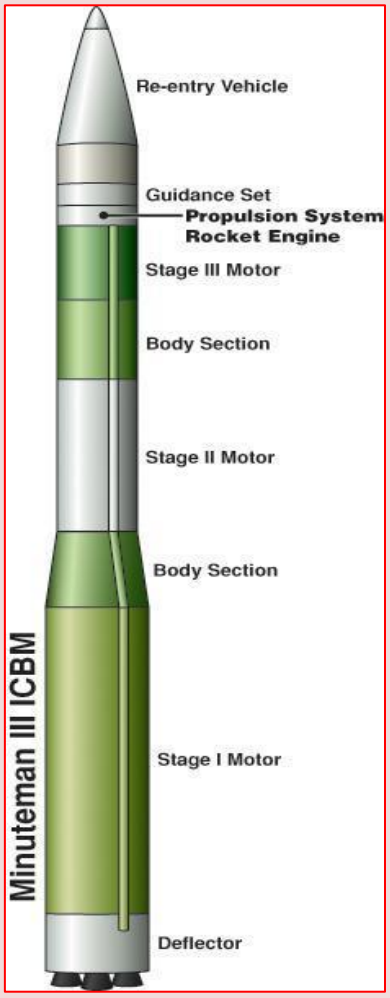
During the same month that Oppenheimer made his remarks, Bernard Brodie, a political scientist at Yale University, proposed a theory of nuclear deterrence that has largely guided American policy ever since. Brodie argued that the threat of retaliation offered the only effective defense against a nuclear attack. "We must do what we can to reduce the advantage that might accrue to the enemy if he hit first," Brodie wrote, after the Soviet Union had obtained its own nuclear weapons. Despite all the money spent on building nuclear weapons and delivery systems, their usefulness would be mainly psychological. "What deters is not the capabilities and intentions we have, but the capabilities and intentions the enemy thinks we have," a classified Pentagon report explained. "The mission is persuasion."

The fear of a surprise attack and the necessity for retaliation soon dominated the strategic thinking of the Cold War. Every year, technological advances compressed time and added more urgency to decision-making. At a top-secret briefing in 1961, Secretary of Defense Robert McNamara was told that a Soviet surprise attack on just five targets—the Pentagon, the White House, Camp David, Site R, and High Point, a bunker inside Mount Weather, Virginia—had a good chance of

wiping out the civilian leadership of the United States. By striking an additional nine targets, as part of a "decapitation" attack, the Soviet Union could kill America's military leadership as well. The Soviets might be able to destroy America's nuclear command-and-control system with only thirty-five missiles. Under McNamara's guidance, the Kennedy Administration sought ways to maintain Presidential control over nuclear weapons. The Pentagon deployed airborne command posts, better communications and early-warning systems, Minuteman missiles that could be quickly launched, and a large fleet of ballistic-missile submarines.

Many of these elements were put to the test during the Cuban Missile Crisis, when a series of misperceptions, miscalculations, and command-and-control problems almost started an accidental nuclear war—despite the determination of both John F. Kennedy and Nikita Khrushchev to avoid one. In perhaps the most dangerous incident, the captain of a Soviet submarine mistakenly believed that his vessel was under attack by U.S. warships and ordered the firing of a torpedo armed with a nuclear warhead. His order was blocked by a fellow officer. Had the torpedo been fired, the United States would have retaliated with nuclear weapons. At the height of the crisis, while leaving the White House on a beautiful fall evening, McNamara had a strong feeling of dread—and for good reason: "I feared I might never live to see another Saturday night."

Today, the United States has four hundred and forty Minuteman III intercontinental ballistic missiles, sitting in underground silos scattered across the plains of Colorado, Nebraska, Wyoming, Montana, and North Dakota. The missiles are kept on alert, at all times, ready to take off within two minutes, as a means of escaping a surprise attack. Each missile carries a nuclear warhead that may be as much as thirty times more powerful than the bomb that destroyed Hiroshima. The Minuteman III was first deployed in 1970 and scheduled for retirement in the early nineteen-eighties. The age of the weapon system is beginning to show. Most of the launch complexes were built during the Kennedy Administration, to house an earlier version of the Minuteman, and some of the complexes are prone to flooding. The command centers feel like a time capsule of late-twentieth-century technology. During a recent visit to a decommissioned Minuteman site, I was curious to see the big computer still used to receive Emergency Action Messages—launch orders from the President—via landline. The computer is an I.B.M. Series/1, a state-of-the-art machine in 1976, when it was introduced. "Replacement parts for the system are difficult to find because they are now obsolete," a report by the Government Accountability Office said last May, with some understatement, about a computer that relies on eight-inch floppy disks. You can buy a smartphone with about a thousand times the memory.



The personnel who command, operate, and maintain the Minuteman III have also become grounds for concern. In 2013, the two-star general in charge of the entire Minuteman force was removed from duty after going on a drunken bender during a visit to Russia, behaving inappropriately with young Russian women, asking repeatedly if he could sing with a Beatles cover band at a Mexican restaurant in Moscow, and insulting his military hosts. The following year, almost a hundred Minuteman launch officers were disciplined for cheating on their proficiency exams. In 2015, three launch officers at Malmstrom Air Force Base, in Montana, were dismissed for using illegal drugs, including ecstasy, cocaine, and amphetamines. That same year, a launch officer at Minot Air Force Base, in North Dakota, was sentenced to twenty-five years in prison for heading a violent street gang, distributing drugs, sexually assaulting a girl under the age of sixteen, and using psilocybin, a powerful hallucinogen. As the job title implies, launch officers are entrusted with the keys for launching intercontinental ballistic missiles.

The Minuteman III is a relic of the Cold War not only in design but also in its strategic purpose. The locations of the silos, chosen more than half a century ago, make the missile useful only for striking targets inside Russia. The silos aren't hardened enough to survive a nuclear detonation, and their coördinates are well known, so the Minuteman III is extremely vulnerable to attack. The President would be under great pressure, at the outset of a war with Russia, to "use them or lose them." The missiles now have two principal roles in America's nuclear-war plans: they can be launched as part of a first strike, or they can be launched when early-warning satellites

have determined that Russian warheads are heading toward the United States. After being launched, a Minuteman III cannot be remotely disabled, disarmed, or called back. From the very beginning of the Minuteman program, the Air Force has successfully fought against adding a command-destruct mechanism, fearing that an adversary might somehow gain control of it and destroy all the missiles mid-flight. "Once they're gone, they're gone," an Air Force officer told "60 Minutes" a few years ago.

The dangers of "launch-on-warning" have been recognized since the idea was first proposed, during the Eisenhower Administration. After the Cuban Missile Crisis, McNamara advised Kennedy that the United States should never use its nuclear weapons until a nuclear detonation had occurred on American soil, and could be attributed to an enemy attack. The first Minuteman missiles had already become a great source of stress for McNamara. The control system of the original model had a design flaw: small fluctuations in the electricity entering the command center could mimic the series of pulses required by the launch switch. An entire squadron of fifty missiles might be launched accidentally without anyone turning a key. "I was scared shitless," an engineer who worked on the system later confessed. "The technology was not to be trusted." McNamara insisted that the control system be redesigned, at great expense. The destruction of fifty Soviet cities because of a mechanical glitch, a classified history of the Minuteman program later noted, would be "an accident for which a later apology might be inadequate."

The launch-on-warning policy became controversial during the nineteen-seventies, once it was publicly known. The hundreds of missiles based on American submarines, almost impossible to find in the depths of the ocean, seemed more than adequate to deter a Soviet attack. During testimony before the House Armed Services Committee in 1979, Fred Iklé, a conservative Republican who later became a top Pentagon official during the Reagan Administration, said, "If any witness should come here and tell you that a totally reliable and safe launch-on-warning posture can be designed and implemented, that man is a fool." The Pentagon repeatedly denied that launch-on-warning was American policy, claiming that it was simply one of many options for the President to consider. A recent memoir, "Uncommon Cause," written by General George Lee Butler, reveals that the Pentagon was not telling the truth. Butler was the head of the U.S. Strategic Command, responsible for all of America's nuclear weapons, during the Administration of President George H. W. Bush.

According to Butler and Franklin Miller, a former director of strategic-forces policy at the Pentagon, launch-on-warning was an essential part of the Single Integrated Operational Plan (SIOP), the nation's nuclear-war plan. Land-based missiles like the Minuteman III were aimed at some of the most important targets in the Soviet Union, including its anti-aircraft sites. If the Minuteman missiles were destroyed before liftoff, the SIOP would go awry, and American bombers might be shot down before reaching their targets. In order to prevail in a nuclear war, the SIOP had become dependent on getting Minuteman missiles off the ground immediately. Butler's immersion in the details of the nuclear command-and-control system left him dismayed. "With the possible exception of the Soviet nuclear war plan, [the SIOP] was the single most absurd and irresponsible document I had ever reviewed in my life," Butler concluded. "We escaped the Cold War without a nuclear holocaust by some combination of skill, luck, and divine intervention, and I suspect the latter in greatest proportion." The SIOP called for the destruction of twelve thousand targets within the Soviet Union. Moscow would be struck by four hundred nuclear weapons; Kiev, the capital of the Ukraine, by about forty.

After the end of the Cold War, a Russian surprise attack became extremely unlikely. Nevertheless, hundreds of Minuteman III missiles remained on alert. The Cold War strategy endured because, in theory, it deterred a Russian attack on the missiles. McNamara called the policy "insane," arguing that "there's no military requirement for it." George W. Bush, while running for President in 2000, criticized launch-on-warning, citing the "unacceptable risks of accidental or unauthorized launch." Barack Obama, while running for President in 2008, promised to take Minuteman missiles off alert, warning that policies like launch-on-warning "increase the risk of catastrophic accidents or miscalculation." Twenty scientists who have won the Nobel Prize, as well as the Union of Concerned Scientists, have expressed strong opposition to retaining a launch-on-warning capability. It has also been opposed by former Secretary of State Henry Kissinger, former Secretary of State George Shultz, and former Senator Sam Nunn. And yet the Minuteman III missiles still sit in their silos today, armed with warheads, ready to go.

William J. Perry, who served as Secretary of Defense during the Clinton Administration, not only opposes keeping Minuteman III missiles on alert but advocates getting rid of them entirely.

"These missiles are some of the most dangerous weapons in the world," Perry wrote in the *Times*, this September. For many reasons, he thinks the risk of a nuclear catastrophe is greater today than it was during the Cold War. While serving as an Under-Secretary of Defense in 1980, Perry also received a late-night call about an impending Soviet attack, a false alarm that still haunts him. "A catastrophic nuclear war could have started by accident."

Bruce Blair, a former Minuteman launch officer, heads the anti-nuclear group Global Zero, teaches at Princeton University, and campaigns against a launch-on-warning policy. Blair has described the stresses that the warning of a Russian attack would put on America's command-and-control system. American early-warning satellites would detect Russian missiles within three minutes of their launch. Officers at NORAD would confer for an additional three minutes, checking sensors to decide if an attack was actually occurring. The Integrated Tactical Warning/Attack System collects data from at least two independent information sources, relying on different physical principles, such as ground-based radar and satellite-based infrared sensors. If the NORAD officials thought that the warning was legitimate, the President of the United States would be contacted. He or she would remove the Black Book from a briefcase carried by a military aide. The Black Book describes nuclear retaliatory options, presented in cartoon-like illustrations that can be quickly understood.

Missiles launched from Russia would give the President about twenty minutes to make a decision, after consultation with the head of the U.S. Strategic Command. The President might have as few as five minutes, if missiles had been launched from Russian submarines in the western Atlantic. A decision to retaliate at once, to launch Minuteman missiles before they could be destroyed, runs the risk of killing millions of people by mistake. A decision to wait—to make sure that the attack is for real, to take no action until Russian warheads began to detonate in the United States—runs the risk losing the ability of the command-and-control system to order a retaliation. In that desperate situation, with the fate of the world in the balance, the temperament of the President would be less important than the quality of the information being offered by the system. Could you trust the sensors?

At about one-thirty in the morning, on October 23, 2010, fifty Minuteman III missiles deployed at F.E. Warren Air Force Base, in Wyoming, suddenly went offline. Launch officers could no longer communicate with their missiles. The letters "LFDN" appeared on their computer screens: Launch Facility Down. Every so often, an underground control center would lose contact with missiles, briefly. It wasn't a big deal. But having an entire squadron go down at once—and remain offline—was a highly unusual event. For almost an hour, officers tried to regain communication with the missiles. When it was reëstablished, remotely, by computer—the control centers are miles away from the missiles—closed-circuit-television images from the silos showed that the fifty missiles were still down there. As a precaution, Air Force security officers were dispatched to all the silos in the early-morning hours.

The Air Force denied that someone had hacked into the computer network and disabled the missiles. A subsequent investigation found that a circuit card, improperly installed in a weapon-systems processor, had been dislodged by routine vibration and heat. The misalignment of the circuit card sent messages to the missiles in the wrong timing sequence. The Minuteman III's complicated launch procedures were designed to allow the missiles to be fired even if some command centers were destroyed, and to prevent rogue officers from firing them without proper authorization. As a result, the fifty missiles in each squadron are connected by coaxial cable to ten control centers, assuring redundancy and enabling one center to veto another's launch decision. Throughout the day, at designated times, each control center sends a signal to the missiles, checks their status, and receives a reply. By disrupting the time sequence, the misaligned circuit board created a cacophony of signals and blocked all communication with the missiles. The system jammed itself.

Although the Air Force publicly dismissed the **threat of a cyberattack on the nuclear command-and-control system,** the incident raised alarm within the Pentagon about the system's vulnerability. A malfunction that occurred by accident might also be caused deliberately. Those concerns were reinforced by a Defense Science Board report in January, 2013. It found that the Pentagon's computer networks had been "built on inherently insecure architectures that are composed of, and increasingly using, foreign parts." Red teams employed by the board were able to disrupt Pentagon systems with "relative ease," using tools available on the Internet. "The complexity of modern software and hardware makes it difficult, if not impossible, to develop components without flaws or to detect malicious insertions," the report concluded.

In a recent paper for the Royal United Services Institute for Defence and Security Studies, Andrew Futter, an associate professor at the University of Leicester, suggested that a nuclear command-and-control system might be hacked to gather intelligence about the system, to shut down the system, to spoof it, mislead it, or cause it to take some sort of action—like launching a missile. And, he wrote, there are a variety of ways it might be done.

During the Cold War, as part of an espionage effort known as Project GUNMAN, Soviet agents managed to tamper with the comb-support bars in sixteen I.B.M. Selectric typewriters at the U.S. Embassy in Moscow and the U.S. Mission in Leningrad. Between 1976 and 1984, every keystroke from those typewriters was transmitted by radio to nearby Soviet listening posts. The tampering was so ingenious that it took twenty-five engineers at the National Security Agency (N.S.A.), working six days a week for several months, with X-ray equipment, to figure out how it was done. Today's integrated circuits contain billions of transistors. As the Defense Science Board notes in its report, a "subversive" chip "could destroy the processor and disable the system by simply shunting power to ground, change the processor output to incorrect results for specified inputs, or allow information leakage to the attackers." A subversive chip would look identical to a normal one.

The cybersecurity of the Minuteman III, aging and yet still on alert, is also questionable. About five thousand miles of underground cable link the control centers to the missiles, as part of the Hardened Intersite Cable System. The cable mainly traverses privately owned land. "One of the difficult parts about fixing missile cable is . . . that the wires are no longer in production," a newsletter at Minot Air Force Base explained a few years ago. The wires are copper, like old-fashioned telephone lines, surrounded by pressurized air, so that attempts to tamper with the cable can be detected. But in the early nineteen-seventies, during Operation Ivy Bells, the United States attached recording devices to similar underwater cable used by the Soviet Navy, tapping into it without piercing it. The mission was accomplished using divers and a submarine, at a depth of four hundred feet, in the Sea of Okhotsk. Digging up part of the Hardened Intersite Cable System in the middle of the night, three to eight feet under a farmer's back yard in Wyoming, would be less challenging. (The Air Force declined to comment on the specific vulnerabilities of the Minuteman III.)

Even if the hardware were pristine, malware could be inserted into the system. During Operation Orchard, in September, 2007, Israel may have hacked into Syria's early-warning system—either shutting it down completely or spoofing it into displaying clear skies—as Israeli fighters entered Syrian airspace, bombed a nuclear reactor, and flew home undetected. In 2012, the Stuxnet computer worm infiltrated computers running Microsoft Windows at nuclear sites in Iran, collected information about the industrial process there, and then issued instructions that destroyed hundreds of centrifuges enriching uranium. A similar worm could surreptitiously enter a nuclear command-and-control system, lie dormant for years, and then create havoc.

Strict precautions have been taken to thwart a cyberattack on the U.S. nuclear command-and-control system. Every line of nuclear code has been scrutinized for errors and bugs. The system is "air-gapped," meaning that its networks are closed: someone can't just go onto the Internet and tap into a computer at a Minuteman III control center. At least, that's the theory. Russia, China, and North Korea have sophisticated cyber-warfare programs and techniques. General James Cartwright—the former head of the U.S. Strategic Command who recently pleaded guilty to leaking information about Stuxnet—thinks that it's reasonable to believe the system has already been penetrated. "You've either been hacked, and you're not admitting it, or you're being hacked and don't know it," Cartwright said last year.

If communications between Minuteman control centers and their missiles are interrupted, the missiles can still be launched by ultra-high-frequency radio signals transmitted by special military aircraft. The ability to launch missiles by radio serves as a backup to the control centers—and also creates an entry point into the network that could be exploited in a cyberattack. The messages sent within the nuclear command-and-control system are highly encrypted. Launch codes are split in two, and no single person is allowed to know both parts. But the complete code is stored in computers—where it could be obtained or corrupted by an insider.

Some of America's most secret secrets were recently hacked and stolen by a couple of private contractors working inside the N.S.A., Edward Snowden and Harold T. Martin III, both employees of Booz Allen Hamilton. The N.S.A. is responsible for generating and encrypting the nuclear launch codes. And the security of the nuclear command-and-control system is being assured

not only by government officials but also by the employees of private firms, including software engineers who work for Boeing, Amazon, and Microsoft.

Lord Des Browne, a former U.K. Minister of Defense, is concerned that even ballistic-missile submarines may be compromised by malware. Browne is now the vice-chairman of the Nuclear Threat Initiative, a nonprofit seeking to reduce the danger posed by weapons of mass destruction, where he heads a task force examining the risk of cyberattacks on nuclear command-and-control systems. Browne thinks that the cyber threat is being cavalierly dismissed by many in power. The Royal Navy's decision to save money by using Windows for Submarines, a version of Windows XP, as the operating system for its ballistic-missile subs seems especially shortsighted. Windows XP was discontinued six years ago, and Microsoft warned that any computer running it after April, 2014, "should not be considered protected as there will be no security updates." Each of the U.K. subs has eight missiles carrying a total of forty nuclear weapons. "It is shocking to think that my home computer is probably running a newer version of Windows than the U.K.'s military submarines," Brown said.

In 2013, General C. Robert Kehler, the head of the U.S. Strategic Command, testified before the Senate Armed Services Committee about the risk of cyberattacks on the nuclear command-and-control system. He expressed confidence that the U.S. system was secure. When Senator Bill Nelson asked if somebody could hack into the Russian or Chinese systems and launch a ballistic missile carrying a nuclear warhead, Kehler replied, "Senator, I don't know . . . I do not know."

After the debacle of the Cuban Missile Crisis, the Soviet Union became much more reluctant to provoke a nuclear confrontation with the United States. Its politburo was a committee of conservative old men. Russia's leadership is quite different today. The current mix of nationalism, xenophobia, and vehement anti-Americanism in Moscow is a far cry from the more staid and secular ideology guiding the Soviet Union in the nineteen-eighties. During the past few years, threats about the use of nuclear weapons have become commonplace in Moscow. Dmitry Kiselyov, a popular newscaster and the Kremlin's leading propagandist, reminded viewers in 2014 that Russia is "the only country in the world capable of turning the U.S.A. into radioactive dust." The Kremlin has acknowledged the development of a nuclear torpedo that can travel more than six thousand miles underwater before devastating a coastal city. It has also boasted about a fearsome new missile design. Nicknamed "Satan 2" and deployed with up to sixteen nuclear warheads, the missile will be "capable of wiping out parts of the earth the size of Texas or France," an official news agency claimed.

The bellicose pronouncements in Moscow suggest that Russia is becoming a superpower again, modernizing its nuclear arsenal and seeking supremacy over the United States. In fact, Russia's arsenal is more inferior today and more vulnerable to a surprise attack than it was forty years ago. The Kremlin's recent propaganda brings to mind some of Nikita Khrushchev's claims from 1959: "Now we have such a stock of missiles, such an amount of atomic and hydrogen warheads, that if they attack us we could raze our potential enemies off the face of the earth." The Soviet Union did not have a single intercontinental ballistic missile when Khrushchev made those remarks.

At the moment, Russia has newer land-based missiles than the United States does, but it also has about a hundred fewer. During the Cold War, Russia possessed hundreds of mobile missiles that were hard to spot from satellites; today, it has only a hundred and fifty, which are rarely moved from their bases and more readily detected by satellite. Russia's ten ballistic-missile submarines now spend most of their time in port, where they are sitting ducks. An American surprise attack on Russian nuclear forces may have the best chance of success since the days of the Kennedy Administration. During the Cold War, as many as five warheads were targeted at each enemy missile to assure its destruction. In an age of cyber warfare, those missiles could be immobilized with just a few keystrokes. The United States Cyber Command—which reports to the U.S. Strategic Command—has been assigned the mission of using "cyber operations to disrupt an adversary's command and control networks, military-related critical infrastructure, and weapons capabilities."

Russia's greatest strategic vulnerability is the lack of a sophisticated and effective early-warning system. The Soviet Union had almost a dozen satellites in orbit that could detect a large-scale American attack. The system began to deteriorate in 1996, when an early-warning satellite had to be retired. Others soon fell out of orbit, and Russia's last functional early-warning satellite went out of service two years ago. Until a new network of satellites can be placed in orbit, the country must depend on ground-based radar units. Unlike the United States, Russia no longer has two separate means of validating an attack warning. At best, the radar units can spot warheads only minutes before

they land. Pavel Podvig, a senior fellow at the U.N. Institute for Disarmament Research, believes that Russia does not have a launch-on-warning policy—because its early-warning system is so limited.

According to Jeffrey Lewis, a nuclear-policy expert at the Middlebury Institute of International Studies, the deficiencies in Russia's command-and-control system feed the country's long-standing fears of encirclement by enemies ready to strike. During the twentieth century, Russia was attacked with little warning by both Germany and Japan. "I think the Russian leadership is terrified of a decapitation strike," Lewis told me recently. "Perhaps some of that is paranoia, but, on the other hand, the United States opened Operation Iraqi Freedom, in 2003, by striking Dora Farm—a failed decapitation strike against Saddam Hussein." Russia's fierce opposition to an American missile-defense system in Europe is driven by fear of the role it could play in a surprise attack. During a crisis, Russia's inability to launch on warning could raise the pressure on a Russian leader to launch without any warning. The logic of a first strike still prevails. As John Steinbruner, a renowned nuclear theorist, explained more than thirty years ago, shooting first "offers some small chance that complete decapitation will occur and no retaliation will follow. . . . [It] is probably the only imaginable route to decisive victory in nuclear war."

Vladimir Putin now wields more power over Russia's nuclear forces than any leader since Khrushchev. Putin has displayed great boldness and a willingness to take risks in foreign affairs. A surprise attack on the United States, given its nuclear superiority and largely invulnerable ballistic-missile submarines, would probably be suicidal. And yet the alternative might appear worse. Putin has described an important lesson he learned as a young man in Leningrad: "When a fight is inevitable, you have to hit first."

For the past nine years, I've been immersed in the minutiae of nuclear command and control, trying to understand the actual level of risk. Of all the people whom I've met in the nuclear realm, Sidney Drell was one of the most brilliant and impressive. Drell died this week, at the age of ninety. A theoretical physicist with expertise in quantum field theory and quantum chromodynamics, he was for many years the deputy director of the Stanford Linear Accelerator and received the National Medal of Science from Obama, in 2013. Drell was one of the founding members of JASON—a group of civilian scientists that advises the government on important technological matters—and for fifty-six years possessed a Q clearance, granting him access to the highest level of classified information. Drell participated in top-secret discussions about nuclear strategy for decades, headed a panel that investigated nuclear-weapon safety for the U.S. Congress in 1990, and worked on technical issues for JASON until the end of his life. **A few months ago, when I asked for his opinion about launch-on-warning, Drell said, "It's insane, the worst thing I can think of. You can't have a worse idea."**

Drell was an undergraduate at Princeton University when Hiroshima and Nagasaki were destroyed. Given all the close calls and mistakes in the seventy-one years since then, he considered it a miracle that no other cities have been destroyed by a nuclear weapon—"it is so far beyond my normal optimism." The prospect of a new cold war—and the return of military strategies that advocate using nuclear weapons on the battlefield—deeply unnerved him. Once the first nuclear weapon detonates, nothing might prevent the conflict from spiralling out of control. "We have no experience in stopping a nuclear war," he said.

During the recent Presidential campaign, the emotional stability of the Commander-in-Chief became an issue, with some arguing that a calm disposition might mean the difference between peace on Earth and a nuclear apocalypse. The President of the United States has the sole power to order the use of nuclear weapons, without any legal obligation to consult members of Congress or the Joint Chiefs of Staff. Ideally, the President would never be short-tempered, impulsive, or clinically depressed. But the mood of the Commander-in-Chief may be irrelevant in a nuclear crisis, given the current technological constraints. Can any human being reliably make the correct decision, within six minutes, with hundreds of millions of lives at stake?

Donald Trump and Vladimir Putin confront a stark choice: begin another nuclear-arms race or reduce the threat of nuclear war. Trump now has a unique opportunity to pursue the latter, despite the bluster and posturing on both sides. His admiration for Putin, regardless of its merits, could provide the basis for meaningful discussions about how to minimize nuclear risks. Last year, General James Mattis, the former Marine chosen by Trump to serve as Secretary of Defense, called for a fundamental reappraisal of American nuclear strategy and questioned the need for land-based missiles. During Senate testimony, Mattis suggested that getting rid of such missiles would "reduce the false-alarm danger." Contrary to expectations, Republican Presidents have proved much more

successful than their Democratic counterparts at nuclear disarmament. President George H. W. Bush cut the size of the American arsenal in half, as did his son, President George W. Bush. And President Ronald Reagan came close to negotiating a treaty with the Soviet Union that would have completely abolished nuclear weapons.

Every technology embodies the values of the age in which it was created. When the atomic bomb was being developed in the mid-nineteen-forties, the destruction of cities and the deliberate targeting of civilians was just another military tactic. It was championed as a means to victory. The Geneva Conventions later classified those practices as war crimes—and yet nuclear weapons have no other real use. They threaten and endanger noncombatants for the sake of deterrence. Conventional weapons can now be employed to destroy every kind of military target, and twenty-first-century warfare puts an emphasis on precision strikes, cyberweapons, and minimizing civilian casualties. As a technology, nuclear weapons have become obsolete. What worries me most isn't the possibility of a cyberattack, a technical glitch, or a misunderstanding starting a nuclear war sometime next week. My greatest concern is the lack of public awareness about this existential threat, the absence of a vigorous public debate about the nuclear-war plans of Russia and the United States, the silent consent to the roughly fifteen thousand nuclear weapons in the world. These machines have been carefully and ingeniously designed to kill us. Complacency increases the odds that, some day, they will. The "Titanic Effect" is a term used by software designers to explain how things can quietly go wrong in a complex technological system: the safer you assume the system to be, the more dangerous it is becoming.

Eric Schlosser *is the author of "Command and Control: Nuclear Weapons, the Damascus Accident, and the Illusion of Safety," from 2013, and a producer of the documentary "Command and Control," from 2016.*

North Korea May Be Cooking Up Flying Uranium Storm

Source: http://i-hls.com/2017/01/north-korea-may-cooking-flying-uranium-storm/

Jan 08 – **North Korea has recently developed a large stealth drone that can carry explosive devices and spread radioactive materials over South Korea,** according to YonhapNews.

"North Korea has begun developing a large drone for reconnaissance and attack purposes in 2012 after its current leader, Kim Jong-un, took power from his late father Kim Jong-il," Kim Heung-kwang, executive director of North Korea's Intellectuals Solidarity (NKIS), said at a press conference held in Seoul.

"The latest drone is **'Banghyun 5'** which was produced at a local airplane repair plant," he added.

The Banghyun 5 is a stealth drone made of titanium and carbon composites. **With a 900-liter fuel tank, the 1.5-ton drone can fly up to 10 hours at a height of 4 kilometers and speed of 200 kilometers per hour,** Kim said.

The North has been improving the stealth functions of unmanned aerial vehicles since 2000. The **Banghyun 5 is designed to deliver a payload of enriched uranium**, which North Korea is believed to possess as a result of its nuclear weapons program.

Also known as a Radiological Dispersal Device (RDD), a dirty bomb is not to be confused with a nuclear weapon. Instead, according to popularmechanics.com, it uses conventional explosives such as TNT or dynamite to spread radioactive material over a wide area. The more powerful the explosive, the wider the contaminated area.

Kim believes that the North intends on using the dirty bomb on South Korea's presidential office and other major facilities or kill key enemy targets, he said.

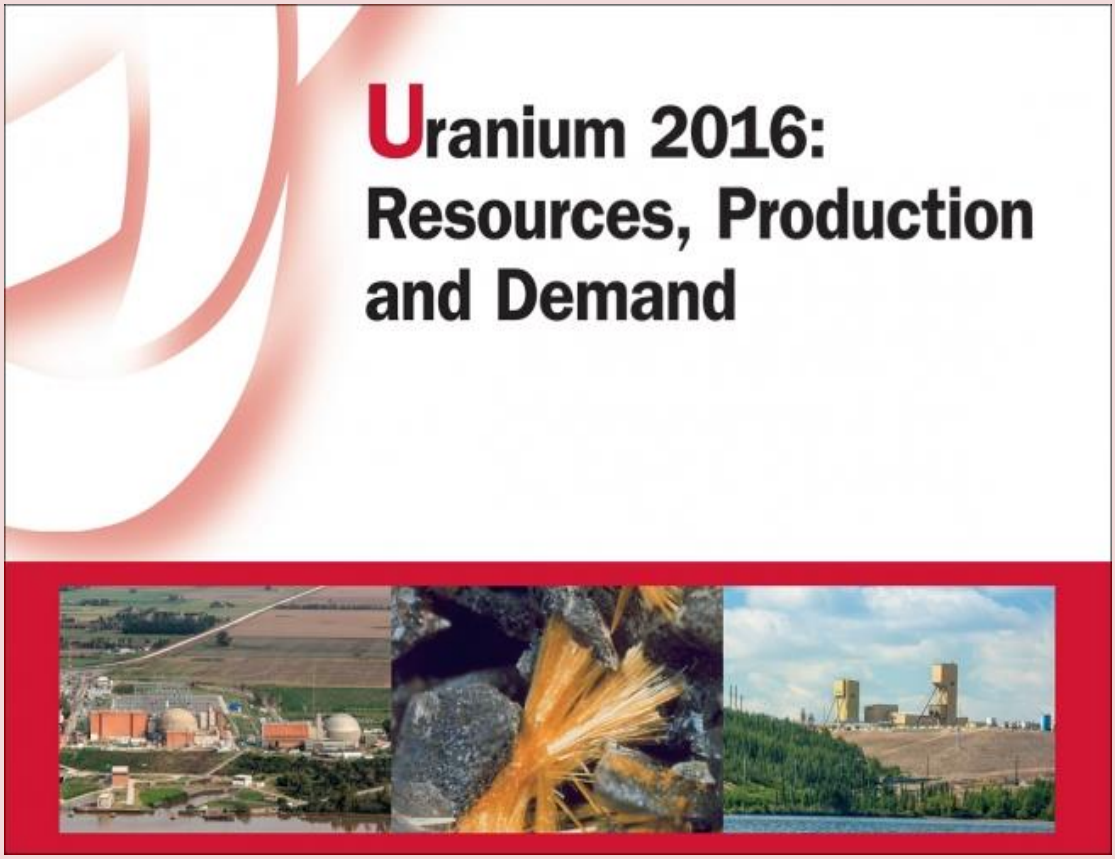
The communist regime has been developing a variety of strategic weapons including an unmanned long-range aerial vehicle that could reach the United States and a nuclear-powered submarine that can carry submarine-launched ballistic missiles, the executive director said.

However, South Korea's military said it does not have any information on the North's development of such advanced drone weapons.

"The specifications of North Korea's unmanned aerial vehicle still lag far behind those of other advanced countries," it said.

New Edition of "Red Book" Uranium Report Is Published

Source: https://www.iaea.org/newscenter/pressreleases/new-edition-of-red-book-uranium-report-is-published



The 26th edition of the "Red Book", a recognised world reference on uranium jointly prepared by the Nuclear Energy Agency (NEA) and the International Atomic Energy Agency (IAEA), was published today. The report provides analyses and information from 49 uranium producing and consuming countries. The new edition provides the most recent review of world uranium market fundamentals and presents data on global uranium exploration, resources, production and reactor-related requirements. It offers updated information on established uranium production centres and mine development plans, as well as projections of nuclear generating capacity and reactor-related requirements through 2035.

Guidelines for Evidence Collection in a Radiological or Nuclear Contaminated Crime Scene

Source: https://www.cbrn-networkofexcellence.org/images/publications/ITWG_Guideline_for_RN_Evidence_Collection_FINAL.pdf

The Nuclear Forensics International Technical Working Group (ITWG) is an informal association of nuclear forensic practitioners, created in 1996 following a G8 summit in Ottawa, Canada, and a subsequent International Conference on Nuclear Smuggling Forensic Analysis held in the United States in 1995. The ITWG aims to provide a framework for combating the illicit trafficking of nuclear materials and other radioactive substances by establishing informal communications and cooperation among international experts, including policy makers, scientists, and law enforcement personnel. In addition, the ITWG Nuclear Forensics Laboratories (INFL) was formed in 2003 to promote technical advancement in the area of nuclear forensics.

The terrifying geography of nuclear and radiological insecurity in South Asia

By Hannah E. Haegeland and Reema Verma

Source: http://thebulletin.org/terrifying-geography-nuclear-and-radiological-insecurity-south-asia10416

This map of India and Pakistan shows: in yellow, nuclear facilities and likely nuclear-capable military bases identified by experts; in red, the known, open-source history of terrorist attacks, incidents of theft, transportation accidents, or personnel reliability program failures involving nuclear or radiological materials and facilities in India and Pakistan; in blue, all terror attacks in India and Pakistan in 2015; and in green, all terror attacks in India and Pakistan in 2014.

Jan 22 – Terrorism involving nuclear or radiological materials remains one of the gravest threats to humanity and to global stability. It was a central concern throughout President Obama's tenure, with efforts to harness international initiatives coming to the fore at the Nuclear Security

Summits. The incoming administration, however, should take a fresh look at a region of the world that hosts two states with nuclear weapons and a serious terrorism problem: South Asia.

Analysis on South Asia tends to occur in silos that focus on either nuclear risks or terrorism risks; fewer studies investigate the overlap between the two.

But we've mapped the geography of high-risk locations and violence by non-state actors—that is, the target threat environment—in South Asia's two states with advancing nuclear weapons programs, India and Pakistan. The low probability but high potential cost of an incident of nuclear or radiological terror merits greater attention from citizens and policy makers alike, and the requisite means, motive, and opportunities for an incident of terror via weapons of mass destruction or disruption converge in South Asia.

The upcoming Summit on Countering WMD Terrorism, to be hosted by India in 2018, offers an opportunity bring attention to the issue. But preparations must begin well in advance of that summit, if the slow-moving machine of bureaucratic change is to be turned to address the institutional and governance problems India and Pakistan exhibit in regard to countering WMD terrorism.

Means to achieve mass destruction or disruption

South Asia is home to expanding and maturing nuclear weapons programs and widespread, frequent, and organized domestic and cross-border terror attacks. Recent incidents include a September 18 assault by terrorists who crossed the border from Pakistan to attack an Indian Army camp at Uri. This incident was followed by Indian retaliation, in the form of a publicly touted "surgical strike." But this clash is one of many. Overall, the region (Afghanistan, Bangladesh, Bhutan, India, Maldives, Nepal, Pakistan, and Sri Lanka) was host to 22,077 terrorist incidents between 2010 and 2015, some 36 percent of the global total. Nearly half of all terrorist attacks in 2015 occurred in four countries: Afghanistan, Iraq, India, and Pakistan. India and Pakistan alone suffered a total of 13,322 incidents and 5,471 fatalities between 2010 and 2015. The Global Terrorism Database at the University of Maryland classified 30 percent of those attacks as armed assaults.

The different modalities of nuclear or radiological terrorism include: an attack on a nuclear facility, theft of nuclear or radiological material and construction of a "dirty bomb," and theft of a nuclear weapon. A fourth, and often overlooked, path by which terrorists could precipitate a nuclear incident is to stage escalatory attacks that draw two states into a nuclear crisis or conflict.

The conditions for all four routes are prime in South Asia's nuclear and radiological threat environment.

The motive for a nuclear or radiological terror attack

A number of violent non-state actors have alluded to their interest in pursuing WMD or precipitating a nuclear event. Some have been even more explicit, demonstrating intent to target a nuclear facility.

Before the 2008 Mumbai terror attacks, for instance, the Lashkar-e-Taiba group is reported to have conducted reconnaissance on India's only plutonium-production facility. The emergence of ISIS in South Asia and the establishment of the Khorasan offshoot, with its wilayat (province) straddling the border of Afghanistan and Pakistan, shows the continued presence of large and sophisticated terror groups that may already have the means, motivation, and capability to acquire sensitive materials.

Reports of ISIS developing a presence in India also continue to surface. One worrying indicator of ISIS' interest in

the destructive potential of nuclear and radiological material became evident in November 2015, when the Belgian police discovered that some ISIS members involved in the Paris attacks had taken hours of surveillance video at the home of an official working at the Belgian nuclear research center with a substantial amount of HEU on-site.

Opportunity for breaking the WMD terror taboo

Pakistan's complicated relationship with domestic and regional non-state actor groups, together with India's lack of an independent nuclear regulatory agency or a comprehensive safeguards agreement for the majority of its declared civilian-use nuclear facilities, highlight vulnerabilities that motivated actors could exploit in the future.

Several documented security blunders connected to nuclear materials and facilities in India over the past two decades raise concerns regarding India's threat environment. In Pakistan, terrorists have carried out direct attacks on facilities believed to have a nuclear weapons role. Some of these incidents are suspected of having being conducted with insider help.

Facilities with the radiological material necessary to create a "dirty bomb" are even more widespread and insecure. While data on Pakistan's radiological material stocks are not readily available, India is one of the largest producers of radiological material in the world. In recent times, India has been searching for a suitable alternative to the isotope cobalt 60 because of its short half-life (i.e. it doesn't stay radioactive as long as other isotopes). India has recently veered towards using cesium 137 as a replacement because of its longer half-life, becoming the first country in the world to use cesium 137 vitrified radioactive sources in the commercial domain. India is estimated to have 57,443 medical X-ray units and more than 12,000 devices that use radioactive materials for industrial and medical applications.

We have created a map of India and Pakistan showing: in yellow, nuclear facilities and likely nuclear-capable military bases identified by experts; in red, the known, open-source history of terrorist attacks, incidents of theft, transportation accidents, or personnel reliability program failures involving nuclear or radiological materials and facilities in India and Pakistan; in blue, all terror attacks in India and Pakistan in 2015; and in green, all terror attacks in India and Pakistan in 2014. From the map, it's clear that sensitive materials and facilities in India and Pakistan suffer from vulnerabilities, and violent non-state actors have demonstrated the capability to carry out attacks on and around these vulnerabilities.

The expanding threat environment in South Asia

Past attacks, thefts, transportation accidents, and personnel reliability issues show that while security failures involving sensitive nuclear materials appear to occur infrequently, they do occur—in both countries. Even more concerning: India and Pakistan are primed to expand their nuclear facilities, production of fissile material, and types of delivery systems, multiplying risks. These expansions make for an even more target-rich environment for motivated non-state actors to exploit. Further, the prevalence of terror attacks in districts where sensitive materials and facilities are located demonstrates that violent non-state actors have demonstrated the capacity (that is, the networks, intelligence, and resources) to reach these areas and threaten hardened targets. While the vast majority of attacks lack sophistication, the low probability but extremely high-risk threat of nuclear and radiological terror highlights the need for swift policy shifts to bolster sensitive material security on the subcontinent.

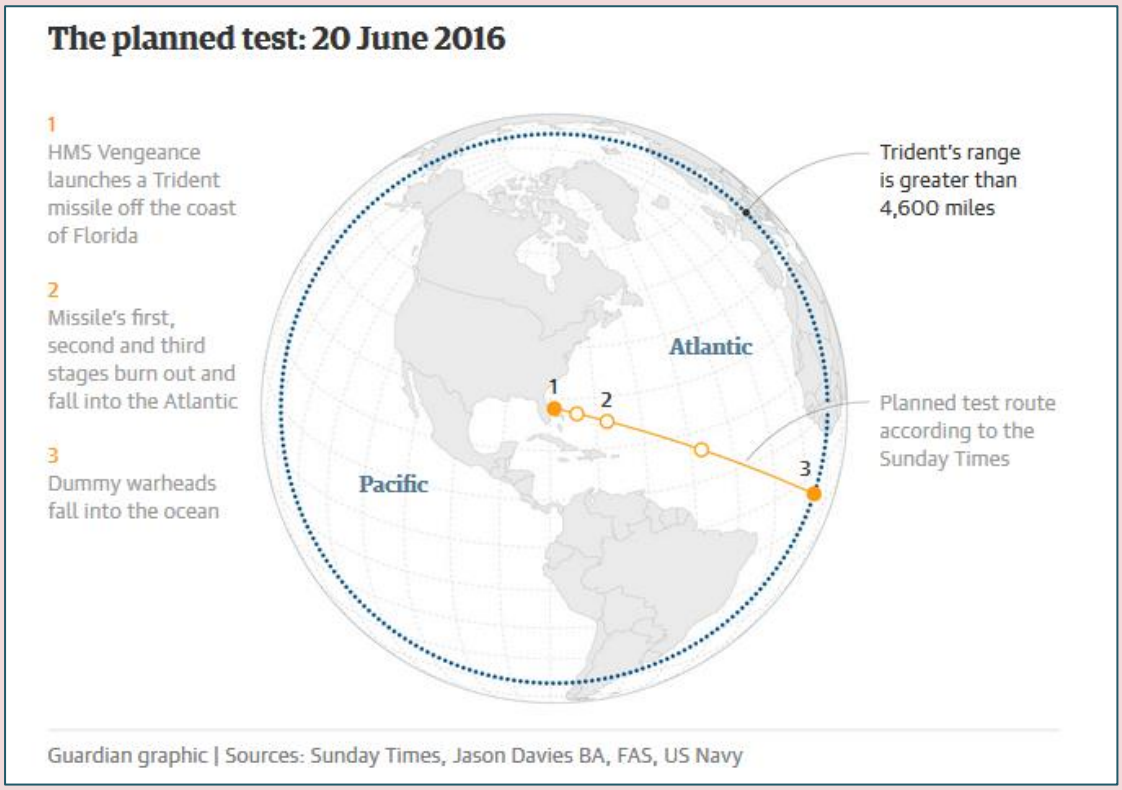
Addressing vulnerabilities to WMD terrorism around the world will take time and concerted policy effort. In 2018, India plans to host a summit on countering WMD terrorism. Preparation for this global initiative will be well served by a serious reevaluation of the geography of nuclear and radiological material security and non-state actor violence in South Asia. In India and Pakistan, we find that the means, motive, and opportunity not only exist but also overlap geographically, revealing an insecure threat environment with the potential for alarming consequences. While nuclear energy trade deals with India have been politically and economically expedient in the last decade, it is dangerous to continue to overlook South Asia's shortcomings in material security. The 2018 Summit in particular is a key opportunity for India to demonstrate regional and global leadership on this issue.

Hannah E. Haegeland *is a research associate in the Stimson Center South Asia Program.*
Reema Verma, *a former Stimson Center South Asia research intern, is completing her graduate studies at George Washington University.*

MoD cannot fall back on usual excuses to explain Trident misfire

Source: https://www.theguardian.com/uk-news/2017/jan/22/mod-cannot-fall-back-on-usual-excuses-to-explain-trident-misfire

Defence departments and arms companies can usually explain away embarrassing failures in the development of new military hardware. There is a ready answer: mistakes are an inevitable part of the process of trial and error at the cutting edge of technology.



But the Ministry of Defence cannot fall back on such an excuse in the catastrophic test-firing of the UK's Trident II D5 ballistic missile in June last year off the coast of Florida. This was not some revolutionary new development still at the experimental stage.

Parcel bomb at far-right bookshop wounds Italian EOD policeman

Source: http://in.reuters.com/article/italy-bomb-idINKBN14L139

Jan 01 – **A parcel bomb with a timer exploded early Sunday morning in front of a Florence bookstore run by a neo-fascist group,** seriously wounding a policeman trying defuse the device, authorities said.

Anti-terrorism police discovered the package while patrolling sensitive sites and called in the bomb squad, Florence police chief Alberto Intini told RAI state television.

The package detonated as a police expert was approaching it at about 5:30 a.m. (04:30 GMT), Intini said.

The officer was rushed to hospital where **his left hand was amputated**, a police source told Reuters. The blast also **left him blind in one eye**, the source said. Police are investigating and would not speculate on who placed the bomb or why.

"It's the third attack in a year on the bookstore," Gianluca Iannone, president of far-right group CasaPound, said in a statement. "It was a clearly political attack," he added.

In the 1970s and '80s, Italy was marred by far-left and far-right extremist attacks. In recent, years such violence has become much less frequent.

The Next Generation of Terror: Swarming, Flying Bomb Robots

By Tobias Burgers and Scott Nicholas Romaniuk

Source: http://nationalinterest.org/feature/the-next-generation-terror-swarming-flying-bomb-robots-18817

Dec 21 - In our prior article we argued that while the United States' overreliance on highly expansive weapon systems, particularly in its fights against terrorists and other violent nonstate actors, is from solely a military perspective the best possible option, from a broader economic, political perspective it is not viable—even self-defeating—in the long term. This argument can, in the wake of recent developments, be extended appropriately to the concept of natural security and the defense of the homeland against threats that would normally fall outside the realm of national military defense, like acts of terrorism of various scale. This article seeks to address the rise of the unmanned terrorism, and seeks to illustrate how exactly this poor man's solution might prove so effective in challenging the notion of security, and as such the political foundation on which Western societies are largely based.

This is particularly true when it comes to providing security for societies under potential threat by "unmanned terrorism"—unmanned aerial vehicles and, possibly in the near future, other unmanned systems too, used for offensive purposes. That is, UAVs with attached improvised explosive devices or the requisite components for chemical, biological, or radiological action against both soft and hardened targets in Western states. The main problem here is defending against a poor man's weapon, as the use of IED UAVs is an extremely cheap method of terrorism, capable of inflicting unprecedented fear. The events of 9/11 alone created lasting psychological trauma in Americans. Now we have to consider the

psychological impact—the spread of fear—across the United States through potentially dozens or even hundreds of much smaller-scale aerial assaults against the U.S. homeland, from a newly contested U.S. airspace.

Protecting against IED UAVs would require wide-ranging means of security, particularly if such systems were to be used together in hybrid attack or swarming strategies in line with the terrorist and insurgent convention of a war without fronts. The threat of swarm attacks—nonlinear dispersed operations—occupies an important position in concepts about the future of warfare and terrorism. Few studies have been conducted on the effects of swarming, and fewer still on how the United States, with its current military and security forces, could successfully defeat enemy swarms. This is despite the fact that enemy swarm tactics have been used in some of recent history's deadliest attacks, like the three-day-long Mumbai terrorist attacks, the militant assault on the Pakistani General Headquarters of the Army in Rawalpindi, and the attack on the Intercontinental Hotel in Kabul. As recently as ten years ago, in-depth research on the concept claimed that swarm attacks could not take place on the ground.

It remains to be seen if security agencies will be able to deal with the possibility of such threats. Rather than focusing solely on a single individual or small groups of militants, they will need to defend against miniature systems coming from the air, sea and land. Compared to suicide terrorism, the practice of IED-UAVs has a further benefit for violent nonstate actors, while also providing new opportunities for U.S. military and security institutions. Those conducting such strikes have the ability to strike repeatedly. In this sense, the IED UAV method is clearly easily repeated, whereas suicide terrorism is undoubtedly a one-time affair, at least for the body acting as the explosive transport.

These scenarios raise concern about security agencies' capabilities, not only to confront these threats, but to do so while considering the financial costs involved. The development of effective countermeasures against such threats has been an area of relatively weak focus, even neglect, on the part of the U.S. military. In principle, defending against such threats would require an enormous increase in manpower, and possibly the development of a new generation of anti-unmanned systems, and the reallocation of both human and nonhuman resources. It further emphasizes the need to mobilize society to be vigilant of new threats from the air—further demonstrating how terrorism and counterterrorism have cultivated the idea of society at war. The question arises whether society would be willing to bear such costs, and possibly more importantly, what would happen if governments are not able to defend against such threats.

Could the era of unmanned terrorism mean that the Hobbesian contract of Western societies is nearing its end, as citizens, concerned with their own security, now seek to rearm themselves against those threats?

Tobias Burgers *is a Doctoral Candidate at the Otto-Suhr-Institute (Free University of Berlin) where he researches the rise and use of cyber, robotic systems in security relations, and the future of military conflict.*

Scott Nicholas Romaniuk *is a PhD Candidate in International Studies (University of Trento). His research focuses on asymmetric warfare, counterterrorism, international security, and the use of force.*

Traces of explosives found on bodies of EgyptAir crash victims

Source: http://news.sky.com/story/traces-of-explosives-found-on-bodies-of-egyptair-crash-victims-10697075

Dec 16 – **Traces of explosives have been found on the bodies of some of the victims recovered from the EgyptAir plane that crashed last May (2016).**

Egypt's Civil Aviation Ministry said in a statement that a criminal inquiry would now begin into the crash of Flight 804.

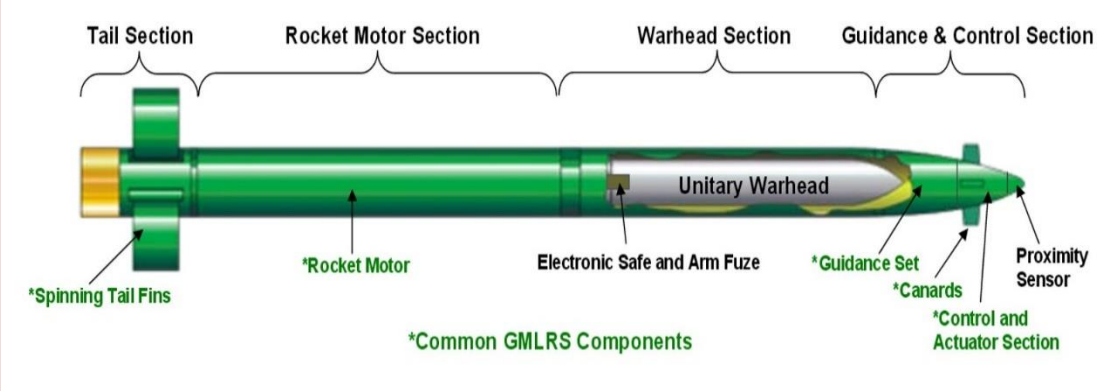
The Airbus A320 plunged into the eastern Mediterranean en route from Paris to Cairo on 19 May, killing all 66 people on board.

Investigators have established a fire broke out in or near the cockpit just before the jet came down between Crete and the coast of northern Egypt.
Sherif Fathy, the country's aviation minister, has said a terrorist attack was the most likely cause.
French investigators said just hours later, however, that it was not possible to draw conclusions on what might have caused the crash.
A spokeswoman for the French BEA said in a statement: "In the absence of detailed information on the conditions and ways in which samples were taken leading to the detection of traces of explosives, the BEA considers that it is not possible at this stage to draw conclusions on the origin of the accident."
The tragedy happened seven months after a Russian airliner crashed in the Sinai Peninsula shortly after taking off from an Egyptian Red Sea resort.
The local affiliate of Islamic State said it had planted a bomb on board and Russia later confirmed there had been an explosion.
There were no survivors among the plane's 226 passengers and crew.

Upgraded Rockets to Hit Targets Without Leaving Unexploded Ordnance

Source: http://i-hls.com/2016/12/upgraded-rockets-hit-targets-without-leaving-unexploded-ordnance/

Dec 29 – **The US Army plans to fire an upgraded, precision-guided, ground-fired rocket which will pinpoint enemy targets at distances up to 70 or more kilometers – while removing the prospect of leaving dangerous unexploded ordnance behind.**
The first **Guided Multiple Launch Rocket System** (**GMLRS**) Alternative Warhead rocket has recently rolled off the production line at Lockheed Martin's manufacturing facility. The GMLRS Alternative



Warhead was designed to engage the same target set and achieve the same area-effects requirement as the old MLRS submunition warheads, but without the lingering danger of unexploded ordnance.

"GMLRS Alternative Warhead rockets are all-weather, time-critical, rapidly deployable guided munitions that return precision area-effects capability to the battlefield commander," said Ken Musculus, vice president of Tactical Missiles at Lockheed Martin Missiles and Fire Control, according to the Lockheed's website.
The weapon is being modified to adhere to the parameters of a 2008 international agreement banning the production and use of so-called "cluster munitions"

which disperse a number of small explosive in an area long after an attack has taken place. This poses risks to civilians who may wind up in the general proximity of areas previously attacked by the rocket.

Primarily designed for fixed targets, GMLRS can be used to destroy enemy bunkers, troop locations, armored vehicles, equipment or other pertinent high-value targets; during the war in Afghanistan, GMLRS was successfully used to destroy senior members of the Taliban, sources have said to scout.com.

GMLRS uses GPS and Inertial Measurement Navigation technology to guide a 200-pound warhead toward dangerous targets; the idea with the new alternative warhead is to use "height of burst" explosion technology to destroy an enemy target through what's called an "area effect," explained Karl Stoetzer, Business Development Manager, Precision Fires, Lockheed Martin.

GMLRS can also fire a "unitary" warhead which can destroy underground targets with a delayed fuse or achieve a proximity or "area effect" similar to the alternative warhead.

It is certainly possible, if not likely, that GMLRS is now being fired against ISIS in Iraq – however the Army quite naturally does not often wish to discuss which weapons are being used on an enemy for operational security reasons.

The GMLRS Alternative Warhead rocket will allow all users of the MLRS to have an area-effects weapon in their inventories without the need to procure additional launcher systems.

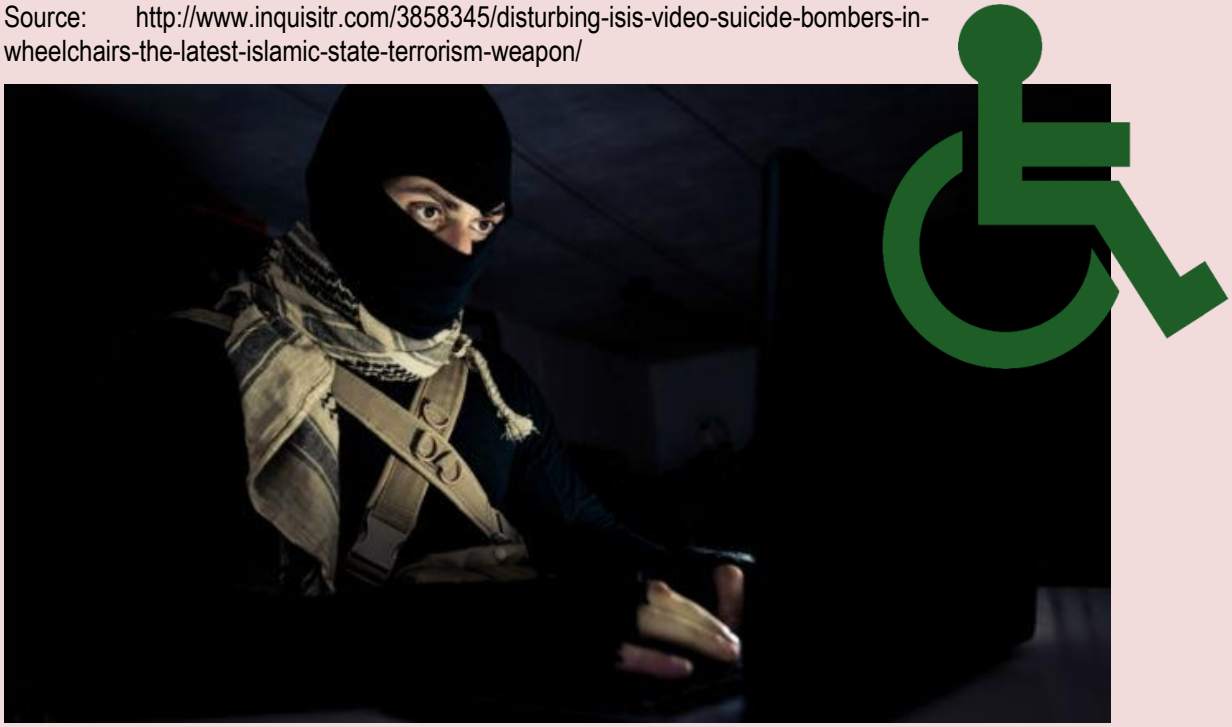
MLRS rockets with submunition warheads ended production approximately six years ago.

Lockheed Martin received the initial production contract from the U.S. Army for GMLRS Alternative Warheads in June 2015.

Each GMLRS Alternative Warhead rocket will be packaged in an MLRS launch pod and will be fired from the Lockheed Martin HIMARS or M270 family of launchers.

Disturbing ISIS Video: Suicide Bombers In Wheelchairs The Latest Islamic State Terrorism Weapon

Source: http://www.inquisitr.com/3858345/disturbing-isis-video-suicide-bombers-in-wheelchairs-the-latest-islamic-state-terrorism-weapon/



Jan 05 – ISIS (Islamic State of Iraq and Syria) extremists have begun using suicide bombers in wheelchairs in their efforts to incite fear and wreak havoc in Mosul, not to mention defend its conquered territory against Iraqi, coalition, and various militia troops attempting to break ISIS' hold on the region. The organization has also posted a video promoting its latest method of terrorist attack. Not only is the footage disturbing, but it presents another challenge for opposing soldiers and even civilians who are inclined to be solicitous toward the disabled to be more wary of a potential danger.

The Daily Express reported this week that ISIS has yet again managed to conjure up a new method by which to outrage humanitarian sensibilities by employing as suicide bombers those whose means of mobility has been relegated to that of a wheelchair. In a video posted by the Islamic State on January 3, suicide bombers in said wheelchairs are seen being readied to carry out various terrorist attacks. The well-produced and professionally presented video also features a series of actions that follow the last moments of a particular suicide bomber.

The ISIS fighter is first seen being helped into his wheelchair before being laden with explosives, apparently for his upcoming mission. The suicide bomber, who has no legs, is interviewed before being wheeled away, implying that he was setting off to perform his mission. The video then cuts to drone footage of an overhead view of a city (believed to be Mosul). A white van-like vehicle (an inset photo of the wheelchair bomber appearing in the bottom right corner to imply he is the driver) is seen moving from one point to another and suddenly disappearing in a billowing cloud of smoke, reportedly the site of a detonated bomb.

ISIS has used the internet to propagandize its efforts in the Middle East as well as proselytize for its brand of radicalized Islam. It should be noted that even though the video of the disabled man might be disturbing to many, the man does not appear to be coerced or forced into becoming a suicide bomber for ISIS. Such is the power of conviction the extremists have for their radical cause. The video itself appears to be an effort to demonstrate that even those that have sacrificed a great deal already still are able to productively benefit the Islamic State and its ultimate goals.

The wheelchair suicide bomber video is believed to be ISIS' first execution video of the year as well. Two men are depicted being executed. One is shown being beheaded on a rooftop. The other is seen being waterboarded before actually being drowned. Both men were accused of spying for the Iraqi coalition.

Although beheading has been a favored execution method for ISIS since its inception, immersing prisoners and captives in water hasn't been the preferred method. Back in May, as was recounted by the *Inquisitr*, ISIS lowered 25 **prisoners into a pool of nitric acid.** And in August, the Islamic State executed six prisoners by boiling them alive in heated vats of burning tar. All were accused of spying for or collaborating with enemy forces.

Of course, the Islamic State has used water before for its executions. As the *Inquisitr* also reported in October, ISIS drowned 58 people in Mosul during one execution event, accusing them of aiding the invading enemy when a plot led by an Islamic State insider was uncovered.

As coalition forces gradually take back the city of Mosul, Iraq, which has been in ISIS control since 2014, the extremists have taken to recruiting terrorists to take the Islamic State's fight to the world. What once was an effort to proselytize and recruit on the internet to get militants to come and fight in the Middle East has turned to efforts to convince converts and members to carry out isolated attacks in their home countries.

The New Year's Eve nightclub attack in Istanbul, Turkey, has now been claimed by ISIS as the work of one of its own. The gunman in that incident went on the shooting rampage, killing 39 people. However, as *CNN* reported, the gunman is still at large and it has yet to be verified if the attacker was actually a member of ISIS.

Drone footage shows ISIS attempt to DECIMATE Mosul with suicide bombers and car bombs

Source (video): http://www.express.co.uk/news/world/750865/isis-Mosul-bombs-cars-suicide-bombers-drone-footage-jihadis

IS blows up major gas plant in Syria's Homs

Source: https://www.alaraby.co.uk/english/news/2017/1/9/is-blows-up-major-gas-plant-in-syrias-homs

Jan 09 – **The Islamic State [IS] group has blown up a natural gas plant that supplied one-third of Syria's electricity,** one month after getting its hands on the facility, a monitor said on Monday.

"In the past 48 hours, IS blew up the Hayyan gas plant in eastern Homs province, putting it totally out of order," said the Syrian Observatory for Human Rights, a Britain-based group that tracks the country's civil war using sources on the ground.

A source at the Syrian oil ministry also confirmed the explosion to *AFP*.

The plant had already ceased to operate one month ago, after the advance of the militants in the central region of Palmyra.

IS on Sunday released a video entitled "Hayyan Gas Company explosion in the east of Homs province" in which a man is seen planting explosives before a wide-angle shot of a huge explosion engulfing the plant.

Jihad Yazigi of the economic news weekly *The Syria Report* said the gas from the plant was used to produce one third of the country's electricity.

According to the weekly, the plant used to produce 3.7 million cubic metres of natural gas per day.

"Therefore millions of Syrians are affected... it was one of the few stations that still produced close to its capacity," Yazigi told *AFP*.

Since 2014, IS has seized several gas and oil fields in Syria, especially in the central and eastern parts of the country.

The US-led coalition regularly carries out airstrikes on oil wells operated by the militants.

Yazigi said the gas from the plant was used to provide electricity for the provinces of Damascus, Hama and Homs, in central Syria.

"The plant represented a large industrial investment and is actually one of the most important... economic infrastructure [facilities] to have been destroyed since March 2011" when the war began, he said

Railway terror alert after staff MISS fake bomb in security test

Source: http://www.mirror.co.uk/news/uk-news/railway-terror-alert-after-staff-9562777

Jan 04 – **A busy rail route running through London has been put on terrorist alert after staff failed to find a fake bomb in a security test.**

The gaff is doubly embarrassing for Govia Thameslink (GTR), which owns Southern Rail, as it is currently locked in a bitter row with rail unions over the "safety critical" role of guards on trains.

The terror alert was issued by GTR to staff on Southern and Thameslink, the Brighton to Bedford line via London, which it also runs.

The train drivers' union Aslef said the incident raised serious concerns over passenger safety at a time when the firm wants to move to driver only-operated trains and downgrade the role of guards.

An internal memo urged staff to be "extra vigilant" after the firm failed a security test in which inspectors from the Department for Transport left an unattended bag containing a 'suspicious item' on a Thameslink train last November.

Tony Holland, GTR's crime and security manager, told staff in the memo:

"Disappointingly, the bag was not found despite being positioned in a public area of the train and railway personnel were seen to walk past the location. This incident further highlights the need for us to be alert and identify any unattended items that may be left on trains and stations. Please remain vigilant at all times."

A spokesman for Aslef said:"How does this reassure passengers. It is quite extraordinary that Southern Railway has failed a DfT security test while getting rid of the guards on trains."

Yesterday the union cut next week's planned six-day strike on Southern Railway, used by 300,000 commuters into London, to three days - January 10, 11 and 13.

But Aslef announced fresh strikes on January 24, 25 and 27 and said the week-long action had been cut because of the impact on the travelling public who have suffered months of disruption caused by staff shortages and industrial action.

Meanwhile,the Southern Railway dispute intensified yesterday with both sides deadlocked over the safety of driver only operated trains.

Aslef accused the government of being behind the dispute and using the Southern as "a battleground" ahead of other train companies, such as Northern and London Midland, planning to bring in driver only operations.

Mick Whelan, Aslef general secretary, insisted the dispute was about safety and not pay and strike action had been taken as a last resort.

He said:"We are taking a longer-term view of this trade dispute. The company has not been prepared to move - it is simply going through the motions.

"We remain committed to a negotiated settlement, as was reached with ScotRail, but it is difficult to negotiate with people who are not prepared to be flexible.

"We still believe a deal can be done but we are, at the moment, a long way from that position. It is time for the company to come up with a genuine offer rather than carry on posturing."

A leaflet will be handed to passengers next week with images of platforms from monitors issued by the company with clear pictures of passengers about to board, compared with photographs taken by drivers which are blurred and dark.

The union said it had raised 50 reported faults with the driver only-operated images seen in the driver's cab since last October, but states:"We continue to raise the same issues and continue to be ignored. We are going around in circles."

Aslef members are operating an overtime ban that is leading to services being cancelled or delayed every day.

The Rail, Maritime and Transport union is also locked in a dispute with Southern over changes to the role of conductors, which has led to a series of strikes.

A Southern spokesman said: "This is a cynical ploy to minimise the impact on Aslef's drivers' pay packets and maximises misery, disruption and hardship for passengers.

"Aslef's move shows pure contempt for the travelling public and it still causes massive disruption over next week.

"These strikes are pointless and they should call the whole thing off and let common sense prevail."

And Rail Minister Paul Maynard said: "Fewer strike days will still

cause massive disruption for passengers. I urge Aslef to call off these wholly unnecessary strikes and come to the table for talks.

"This modern way of running trains has been safely used elsewhere in the UK for 30 years. There is no safety issue; the independent rail regulator has confirmed it is safe."

Ethiopia: Bomb explosion hit a hotel in Bahir Dar

Source: https://ethsat.com/2017/01/ethiopia-bomb-explosion-hit-hotel-bahir-dar/

Jan 04 – **A grenade explosion** hit the Grand Hotel in Bahir Dar Wednesday night, eyewitnesses told ESAT.

No party claimed responsibility for the explosion that happened at 8:00 p.m. local time. No casualties have been reported so far.

There has been a campaign against the staging of a musical concert at the Hotel by the locals who said the city is still mourning the death of hundreds residents shot and killed by security forces during anti-government protests this summer.

Witnesses also said there were government officials at the Hotel at the time of the explosion.

The owner of the Grand Hotel, Tiliksew Gedamu, is believed to have close ties to ruling party officials.

US Army searching for technical approaches and potential technical solutions to counter the threat from Anti-helicopter Mines and Improvised Explosive Devices (IEDs)

Source: http://counteriedreport.co.uk/news/us-army-searching-for-technical-approaches-and-potential-technical-solutions-to-counter-the-threat-from-anti-helicopter-mines-and-improvised-explosive-devices-ieds

Jan 03 – The purpose-built anti-helicopter mines and IEDs are far more sophisticated and dangerous.These are not regular land mines buried in the ground, but sophisticated, radar-controlled air

defence weapons that have been developed by several nations.

The US Army specifically cites "the fielding of anti-helicopter mines by Russia and Bulgaria." Bulgaria, which seems to have developed these devices as far as as the late 1990s, offers several mines such as the AHM-200. The mine, which is emplaced on the surface rather than buried in the dirt, has an acoustic sensor which arms the weapon when it picks up the sound of the helicopter as far away as 1,500 feet. At a range of 500 feet, a Doppler radar tracks the target. When the helicopter gets within 300 feet, the mine detonates both an explosively formed projectile and an explosive charge packed with steel balls.

A 2012 Russian news video shows what looks like a similar device.

Poland has developed a mine that effectively fights helicopters that come within a range of up to 150m at a speed up to 300 km/h (http://readgur.com/doc/1289364/anti-helicopter-mine—wojskowe-zak%C5%82ady-uzbrojenia-sa), and Austria has developed the anti-helicopter mine that uses an Infrared sensor and an acoustic sensor to detect airborne targets (https://en.wikipedia.org/wiki/Helkir_mine).

The US Army's Anti-Helicopter Mine and Improvised Explosive Device Countermeasures project will have three phases:

- **PHASE I:** Phase I will consist of a feasibility study which includes an overview of relevant historical and technical data. The study will identify technical and tactical characteristics of current and emerging Anti-Helicopter Mines and IED threats, to include fuzing, kill mechanisms and employment techniques. Finally, the study will identify potential innovative countermeasures, including their current technical maturity and their tactical and technical advantages and disadvantages.
- **PHASE II:** Phase II will consist of the vendor providing a developmental prototype of the preferred approach, identified in Phase I, for testing against a variety of anti-helicopter mines and IEDs in conjunction with one or more rotary wing aircraft in an operational flight profile.
- **PHASE III:** Phase III will consist of the vendor providing a technology demonstrator that incorporates the lessons learned from testing and analysis conducted in phase II. This technology demonstrator will be used to support the establishment of a program of record through the requirements development process of the US Army and other interested elements of the Department of Defense.

Vehicle Ramming Attacks – Are There Any Security Measures?

Source: http://i-hls.com/2017/01/vehicle-ramming-attacks-security-measures/

Jan 09 – A terrorist attack carried out by a lorry driver ramming into the crowd is very hard to prevent, it can cause untold damage and seemingly comes out of nowhere. The Bastille Day attack in Nice killing dozens of people, the Berlin Christmas market lorry attack and yesterday's lorry attack in Jerusalem are a few examples.

Various technological solutions are sought, including attempts to develop a technology to remotely stop high-risk vehicles.

According to the guardian.com there are several measures police can take in order to lower the risk of such attacks.

The primary way is to erect huge barriers around vulnerable crowded areas: indeed, police chiefs in Berlin said after the attack they would now plan to do this.

In Britan, the most obvious form of protection against a truck attack is large barriers. The black barriers around the Palace of Westminster are designed to stop a lorry attack at high speed.

All US military and governmental buildings have "crash- and attack-resistant bollards" outside. The US state department "anti-ram vehicle list" lists several types of bollards to protect the perimeter of its embassies abroad. Some bollards are capable of stopping vehicles traveling at up to 50mph (80km/h).

There are also innovative ways of protecting large crowds. Arsenal's Emirates Stadium has been held up as a model for how physical barriers can be incorporated into a building's design. Large concrete letters spelling out the word Arsenal at the stadium's main entrance also act as a barrier to vehicles. Concrete benches prevent a vehicle from weaving across the forecourt, and giant ornate cannons, which feature on the club's logo, form an obstacle for vehicles driving towards the stadium building.

Measures also include tight bends and restricted-width streets to prevent a large vehicle building speed before reaching a bollard or barrier.

In the 2007 Glasgow airport attack, the concrete bollards outside the airport were credited with stopping the vehicle entering the terminal, although the terminal doors were damaged.

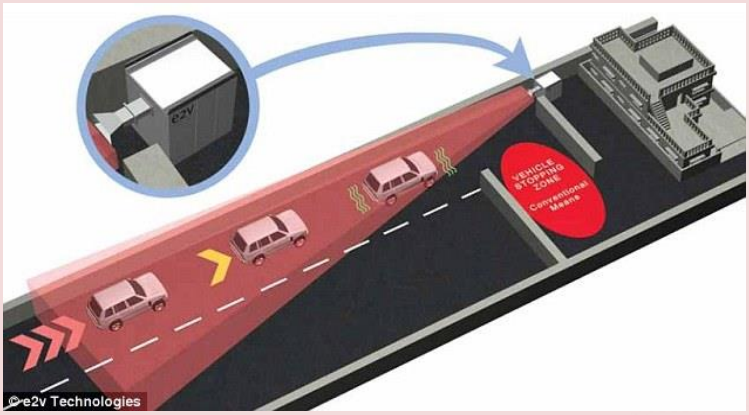
The attack in Glasgow prompted a government review of the protection of strategic infrastructure, which recommended the installation of robust physical barriers as protection against vehicle bomb attacks and the creation of vehicle exclusion zones to keep all but authorised vehicles at a safe distance.

Prof Tahir Abbas, a senior research fellow at the Royal United Services Institute, said many important government buildings and public sites in Britain were already surrounded by barriers to stop vehicle attacks, however, "when you have an open event, something that's almost ad hoc such as a Christmas market, then the need to have greater security measures has become more pronounced," he said.

"Now designers and scientists have got the technology to create aesthetically pleasing barriers to prevent cars from ramming into buildings," said Abbas. "As part of that you have things like innocent flower pots outside buildings that are actually enforced with concrete and metal to prevent a truck from going over them. They are hidden and blended into the aesthetics of the building."

Project Restore

Experts in the UK Home Office's scientific wing want to develop and install a technology which would enable them to stop high risk vehicles remotely. These include HGVs and other large vehicles, particularly those carrying hazardous loads such as fuel and chemicals.



Known as **Project Restore**, which stands for the **REmote STOpping of Road Engines**, they are also setting minimum standards for the innovation.

'Law enforcement are looking at the technical ability to immobilise vehicles when criminals misuse them,' said one senior official. `This would have the added benefit of increasing the security of vehicles making them more difficult to steal. It also gives police an additional option for stopping a moving vehicle and regaining control without the use of firearms.'

It seems that the problem is that stinger-type devices do not work on large vehicles so there needs to be another way of stopping or slowing a vehicle down.
According to the Daily Mail, landmark buildings, transport hubs and public buildings are already protected by heavy concrete bollards and gates designed to prevent access in a Nice-like scenario. Temporary measures to seal off streets are also used during major public events such as the Notting Hill Carnival and Royal celebrations. Police advisors fear it could be all too easy for a terrorist to hire or steal an HGV, or even pose as a bogus employee.
Earlier this year, Scotland Yard boss Sir Bernard Hogan-Howe said he would like to be able to switch off all vehicles, including mopeds, remotely.
'My ideal scenario would be that we'd have a device that slowed down the car in front,' he said.
'It may sound far-fetched but these things can be developed and, of course, now cars have got more electronic brains, so that for me that would be a great opportunity to safely slow down the vehicle.'
It is not the first time that policing agencies have investigated a 'kill switch' for cars, and similar devices are already available in the private sector. **Two years ago it was revealed that the European Union is secretly developing the technology as part of wider law enforcement surveillance and tracking measures.** A leaked document said the technological solution would become a 'build in standard' for all cars that enter the European market.
It could be activated from a police worker monitoring the movement of the vehicle via GPS from a control centre.
'Cars on the run can be dangerous for citizens,' said the document. 'Criminal offenders will take risks to escape after a crime. 'In most cases the police are unable to chase the criminal due to a lack of efficient means to stop the vehicle safely.'

GERMANY TERROR: Police seize 155 KILOS of EXPLOSIVES and arrest two with 'neo-Nazi links'

Source: http://www.express.co.uk/news/world/754114/German-police-155-kilos-explosives-two-men-arrested-terrorist-right-wing-links

Jan 14 – **German police have detained two men suspected of having links to a terror group after seizing 155kg of explosives**.
Prosecutors in Germany investigating the arrest of two men for possession of 155kg of explosives have said the pair used contacts within the right-wing scene.

The two men, aged 18 and 24, were detained in October last year for possession of explosives and were being questioned over possible links to the Neo-Nazi terrorist group Oldschool Society (OSS).

Lauterecken

According to the report the teenager had confessed to a meeting with the OSS in the summer last year in a hut in Rhineland-Palatinate.
The report, seen by Die Spiegel, quoted the 18-year-old as saying a participant at the meeting had said: "One has to do something in Germany" and asked if anyone could produce 250kg of explosives for him.
Both arrested men deny that they planned any attack but had the explosives, mostly

comprising illegal fireworks, for their own private use.
According to the "Spiegel", however, a self-constructed explosive set with a Hakenkreuz and SS-Runen was also found during the search of the 18-year-old parental home at the beginning of January.
The 24-year-old presumed accomplice from North Rhine-Westphalia had come to the police's attention, according to "Spiegel" years ago.
In 2012, investigators also found right-wing literature in his possession.
In the ongoing investigation, however, no evidence of a right-wing leanings were found, according to the newspaper, referring to investigative circles.
The authorities are still investigating whether he and the 24-year-old had planned an attack in Kaiserslautern.
The investigation is ongoing.
The men were held after a special forces raid on an apartment in the German town in the south-west of the country in October.
Police seized 155kg of explosives and an improvised explosive device which were reportedly marked with a swastika and SS signs.
Saxony Police spokesman Tom Bernhardt said at the time that the explosives were "relatively well hidden".

WHO condemns reported attacks using ambulances as weapons targeting civilians in Tikrit and Samarra, Iraq

WHO statement
6 November 2016
Source: http://www.who.int/mediacentre/news/statements/2016/attacks-using-ambulances/en/

WHO condemns reported attacks using ambulances to target civilians in Tikrit and Samarra. WHO received reports of suicide bombers driving ambulances, killing more than 20 people and injuring dozens more at a checkpoint in Tikrit and a car park in Samarra. The reported use of medical vehicles as weapons threatens the ability to deliver health care and urgent medical services. When ambulances are suspected as potential security threats, their freedom of movement to care for the sick and injured is at risk of life-threatening delays. Such delays will leave vulnerable people with even less access to life-saving medical care.

WHO is increasingly concerned by the continuous threats to health workers, facilities and transport. WHO is working together with national health authorities and partners to protect patients, health workers, health infrastructure and supplies from violence and thus minimize disruptions to desperately needed health care.

At least 32 Jewish Community Centers targeted in second wave of bomb threats

Source: http://www.homelandsecuritynewswire.com/dr20170119-at-least-32-jewish-community-centers-targeted-in-second-wave-of-bomb-threats

Jan 19 – At least 32 Jewish Community Centers across the United States were subjected to bomb threats on Wednesday, less than ten days after sixteen more JCCs were evacuated after similar threats. JCCs and other Jewish institutions were targeted in the Boston, Miami, Detroit, Cincinnati, Nashville, Minneapolis, and Orlando metro areas, among others. The Anti-Defamation League says that anti-Semitic incidents have spiked since the presidential election.

The worst cyber attacks of 2016

Source http://m.economictimes.com/small-biz/security-tech/security/the-worst-cyber-attacks-of-2016/articleshow/56212448.cms?utm_source=facebook.com&utm_medium=referral&utm_campaign=ETFBMain

Dec 28 – From leaking debit card details to influencing the US Presidential Election, have become a significant part of our political and social discourse. ET's Nilesh Christopher takes a look at the top hacks of the year.

Indian Debit Card Hack

Who? Unknown
What? As many as 32 lakh debit cards belonging to various Indian banks were compromised earlier this year resulting in the loss of Rs 1.3 crore in fraudulent transactions as per NPCI.
The hacks went undetected for months, and reports suggest ATMs operated by Japanese Hitachi Payments were infected with malicious software allowing hackers to extract money off user accounts.

Legion Hacks (India)

Who? The legion crew
What? Infamous hacker group Legion made headlines in the sub-continent after hacking into the Twitter accounts and partial email dumps of prominent public figures such as politician Rahul Gandhi, businessman Vijay Mallya, and NDTV journalists Barkha Dutt and Ravish Kumar.
The group gave details of upcoming hacks, romanticised the use of drugs and promised to come out with more dumps in the coming days.

Bangladesh Bank Hacks

Who? Unknown
What? One of the largest financial crimes executed online took placein early February when $81 million of Bangladesh's money was siphoned off by unknown hackers, reportedly to Philippines, Sri Lanka and parts of Asia.

Dyn Cyber Attack

Who? Hacker groups anonymous and new world hackers claimed responsibility
What? The largest cyber attack in recorded history happened on October 21, causing temporary shutdown of websites such as Twitter, Netflix, Airbnb, Reddit, SoundCloud, etc. The three-fold hack caused mass internet outage for large parts of the US and Europe.
Servers of Dyn, the company which controls the lion's share of the internet's domain name servers (DNS) were attacked, which largely affected internet of things (IoT) devices.

Philippines Voter Data Leak

Who? Hacker groups Anonymous Philippines and Lulsec
What? Philippines suffered its worst-ever data leak when hackers divulged personal information of voters including fingerprint data and passport information of 70 million voters. The entire database of 340 GB of Philippines commission on the election (Comelec) was leaked online.

Russian Interference in US Elections

Who? Russian hackers
What? Russians hacked into the Democratic National Convention (DNC), influencing the election in favour of Donald Trump. The hackers, it is said, sent out repeated phishing emails to various US institutions before John Podesta, the chairman of

Hillary Clinton's campaign clicked on one of the malicious mails allowing access to over 60,000 emails of the Clinton campaign.
Reports suggest the emails were forwarded to WikiLeaks website, which later published those mails in the run up to the US Elections tainting Clinton's image further.

Yahoo Data Theft
Who? Unknown
What? Yahoo! reported two major data thefts this year: The first in September which affected over 500 million Yahoo! user accounts, and another in December which said one billion accounts were compromised. User names, email addresses, date of birth, passwords, phone numbers, and security questions were all leaked.

Mark Zuckerberg Hack
Who? OurMine security group
What? Facebook cofounder Mark Zuckerberg's Twitter and Pinterest accounts were breached multiple times this year, because he reused a password "dadada".
OurMine hacks into celebrity accounts to advertise their commercial services and even claimed responsibility for hacking into Sundar Pichai's Quora account in June.

Oracle MICROS Hack
Who? Russian hacking group
What? A Russian hacker group notoriously known for hacking banks breached into the computer network of Oracle, compromising their MICROS point-of-sale credit card payment systems. MICROS is among the top three point-of-sale vendors globally.

The Top 17 Security Predictions for 2017

By Dan Lohrmann
Source: http://www.govtech.com/blogs/lohrmann-on-cybersecurity/the-top-17-security-predictions-for-2017.html

Dec 27 –**"You ain't seen nothing yet!"**
That's the collective view from global cyberexperts as they describe the coming year of new data breaches and technology disruption that will impact every area of life.
As we exit 2016, a year in which hackers stole the show for a variety of causes, cybersecurity has risen to the top of the international priority list in areas ranging from politics to national defense and from smart homes to our global economic system. With new drones, artificial intelligence, social media websites, robots, autonomous cars, smart city infrastructure, and a plethora of Internet of Things (IoT) devices coming onto the market daily, how can we prepare for next-generation cyberattacks?
At the beginning of this year, I answered the question: Why more security predictions and how can you benefit? At the end of that article, I told readers to expect even more security predictions as we head into 2017. That has turned out to be true — with a twist.
No doubt, there are more lists looking toward the future than ever before. As I examined hundreds of technology and security articles, blogs, slideshows, videos and infographics related to upcoming 2017 events, I've seen a growing number of organizations prefer to name their views on the coming year as "forecasts" or "trends" or "projections." I suppose that a "forecast" does sound more scientific — like a weather forecast that is based on mathematical models, satellites, radar and much more.
What is quite clear is that these lists contain a wide variety of content that ranges from hopes (you might even call them New Year's resolutions based on what vendors are already working on) to connecting-the-dots threat projections (based on 2015 and 2016 data) to educated guesses on security to dramatic cyberspeculations that get media attention. Security predictions are also showing up on other lists from automobile announcements to defense spending to the home toy market.
Nevertheless, I maintain my view that the security and technology industries offer tremendous value with these cyber research reports and expert analysis on threats from their best and brightest. I strongly urge technology and security pros to review these

referenced lists and check them twice, in order to improve your strategic plans, product road maps, incident response scenarios and overall business operation.

For background and comparison purposes, here's a reminder of the top 15 security predictions for 2015 and the top 16 security predictions for 2016. On a personal level, understanding online risk trends within your industry is a must for ongoing career growth and maintaining security thought-leadership as well as to enable workable technology solutions.

So here's my "Guide to 2017 Security Predictions," for readers who want to see the specific company prediction details as we head toward New Year's Day 2017. If you want to jump to conclusions, my cyberprediction award-winners follow at the end.

The Top 17 Security Predictions by Company

1) Symantec — The three lists of predictions that are offered by Symantec are very similar to the lists offered by others, so I offer them here (with details at their website):

Cloud Generation dynamics define the future of the enterprise

- The enterprise network will expand and become increasingly undefined and diffuse.
- Ransomware will attack the cloud.
- AI/machine learning will require sophisticated big data capabilities.

Cybercrime becomes mainstream

- Rogue nation states will finance themselves by stealing money.
- Fileless malware will increase.
- Secure Sockets Layer (SSL) abuse will lead to increased phishing sites using HTTPS.
- Drones will be used for espionage and explosive attacks.

IoT comes to enterprise business

- The proliferation of the Cloud Generation.
- IoT devices will increasingly penetrate the enterprise, leading to increased IoT DDoS attacks.

2) Trend Micro — The list of eight security predictions offered by Trend Micro doesn't contain any "wows," but the explanations are again very helpful, offering in-depth explanations. Unlike some other companies, they think ransomware will plateau, but "attack methods and targets will diversify."

They also predict that "Adobe and Apple will outpace Microsoft in terms of platform vulnerability discoveries."

They also call out increasing "cyberpropaganda" as the use of tools and methods to influence elections and public opinion. "Most recently, we have seen platforms like WikiLeaks used for propaganda — with highly compromising materials leaked through the site just a week before the US elections. In our continuous monitoring of the cybercriminal underground, we also noted script kiddies advertise their earnings from fake election-related news. They claim to make around US$20 per month by driving traffic to fabricated smear content about electoral candidates."

3) McAfee — This excellent white paper (in PDF format) offered by McAfee covers a wide range of trends and 2017 predictions that are worth noting. Here are a few highlights from their 14 predictions:

- Ransomware will remain a very significant threat until the second half of 2017. Ransomware-as-a-service, custom ransomware for sale in dark markets, and creative derivatives from open source ransomware code will keep the security industry busy through the first half of the year. Ransomware's impact across all sectors and geographies will force the security industry to take decisive actions. We predict that initiatives like the No More Ransom! collaboration, the development and release of anti-ransomware technologies, and continued law enforcement actions will reduce the volume and effectiveness of ransomware attacks by the end of 2017.
- "Dronejacking" places threats in the sky
- IoT malware opens a backdoor into the home
- Machine learning accelerates social engineering attacks
- The explosion in fake ads and purchased "likes" erodes trust
- Hacktivists expose privacy issues
- Threat intelligence sharing makes great strides

4) Forcepoint — There are 10 Forcepoint predictions, and like many other companies, they offer a webcast and a downloadable document with details. A few of their highlights include:

- Compliance & Data Protection Convergence — 2017 will be the final full year before the European Union's (EU) General Data Protection Regulation (GDPR) is a legal requirement. GDPR demands may drive business costs higher as new data protection controls are applied and multiple stakeholders grapple with the who, when and how of data accessibility requirements.
- Rise of the Corporate Incentivized Insider Threat — A new corporate-incentivized insider threat may clash with customer data, corporate profit and other performance goals, forcing businesses to re-evaluate their corporate environments and growth strategies.
- Voice-first Platforms & Command Sharing — The rise of voice-activated AI to access Web, data and apps will open up creative new attack vectors and data privacy concerns.

5) FireEye — A slightly different approach was taken by FireEye this year. They offer good questions and related answers regarding 2017. Here are a few highlights:

"In 2017, cyber security battles may favor criminals even more as the Internet of Things (IoT) continues to expand possible avenues of attack. The 2017 security predictions from FireEye include insights on:

- What investments security organizations will make in 2017**.** Security integration and orchestration should be considered the benchmarks of new technology investment.
- Which industry or type of organization might unexpectedly become a target of threat groups in 2017? Religious institutions in Western countries are at the top of the list because they typically lack a robust security program yet maintain contact information and other sensitive data.
- How threat groups will continue to target industrial control systems (ICS) in the near future? A recent report revealed that security patches were not yet available for more than 30% of identified ICS vulnerabilities."

6) Kaspersky — Kaspersky Lab predicts that 2017 will continue to see the commodification of financial attacks.

"The commodification of attacks along the lines of the 2016 SWIFT heists — with specialized resources being offered for sale in underground forums or through as-a-service schemes, will continue in 2017. As payment systems become increasingly popular and common, this will be matched by a greater criminal interest next year.

As far as ransomware is concerned, Kaspersky Lab also anticipates the continuing rise of ransomware, but with the unlikely trust relationship between the victim and their attacker — based on the assumption that payment will result in the return of data."

7) Palo Alto Networks — The list of Palo Alto predictions for 2017 is impressive. Their items are divided into "sure things" and "longshots." They cover many cyberareas, including our cybertalent shortage.

- A few 'sure things' include: "Recruiters Search for Cyber Talent Outside of Security" and "The need for non-technical security professionals will also increase."
- Longshots include: "Companies acquire other organizations to inherit talent."

8) Watchguard Technologies — I really like the various 2017 prediction offerings via several channels from Watchguard Technologies. They offer creative predictions, infographics, YouTube videos on their top predictions and more. Here are two examples:

- First on their Watchguard list is Ransomworm, and this video below describes what that means. They also describe IaaS as an attack platform and surface and new steps in a global cyberwar leading to a civilian casualty.
- I also like this infographic listing 2017 predictions from Watchguard Technologies.

9) Imperva — There has consistently been a good list of predictions from Imperva over the years. This year they offer**:**

- Botnet of Things

- Ghosts from the past
- Cyber Fatigue

10) Beyond Trust — There are 10 cybersecurity predictions offered by BeyondTrust. They lead with this bold item: **"**The first nation state cyber-attack will be conducted and acknowledged as an act of war."
They also list Tor v2, cloud-based attacks, and: **"**Behavioral technologies, such as pressure, typing speed and fingerprints, will be embedded into newly-released technologies."

11) Checkpoint — There are Checkpoint predictions for mobile, industrial Internet of Things (IIoT), critical infrastructure, threat prevention and the cloud from Checkpoint. "An attack to disrupt or take down a major cloud provider will affect all of their customers' businesses. While generally disruptive, it would be used as a means to impact a specific competitor or organization, who would be one of many affected, making it difficult to determine motive. There will also be a rise in ransomware attacks impacting cloud-based data centers."

12) Forrester — The list of 2017 predictions from Forrester covers every major enterprise area, but details need to be purchased. In the cybersecurity area, they predict that risks will intensify. They also say, "Security And Skills Will Temper Growth Of IoT." (Note that both Gartner and Forrester are using these predictions as lures to buy their more in-depth prediction analysis.)

13) Gartner — Always known for their ability to put next percentages next to their predictions, Gartner offered these free security predictions regarding the next 2-4 years several months back. More recently, Gartner offers these free mobile security predictions — with advice attached.

- The first significant finding in the report is that, "Mobile attacks (Pegasus, XcodeGhost) and vulnerabilities (Stagefright, Heartbleed) are increasing in terms of both number and pragmatism.
- Now is the time to start your Mobile Threat Defense (MTD) initiative.
- No EMM? Mobile Threat Defense protects employees and eliminates privacy concerns.

14) White Hat Security — Some very interesting predictions here, including this one from Dan Lacey: *Nothing will change.* "Attackers will continue to discover and exploit zero-days. Companies large and small will continue to lose data and money to the usual attacks, often because they didn't take basic security precautions. Individuals will continue to lose money in the usual ways, often because they lack basic knowledge of Internet safety. Manufacturers will continue to produce Internet-connected devices with no security, or easily by-passable security, enabling attackers to hijack them. Someone might pass laws mandating that new Internet of Things devices have security, but those laws will be unenforceable and impossible to apply retroactively. No one will deploy a better authentication system than passwords."

15) Sophos — Here is another example of cybersecurity trends for 2017 from Sophos, which reads a lot like other lists, staring with: **"**Destructive DDoS IOT attacks will rise."
- But at the same time, they offer this on encryption's downside: "As encryption becomes ubiquitous, it has become much harder for security products to inspect traffic, making it easier for criminals to sneak through undetected. Unsurprisingly, cybercriminals are using encryption in creative new ways. Security products will need to tightly integrate network and client capabilities, to rapidly recognize security events after code is decrypted on the endpoint."

16) IDC – And if you are not depressed yet, IDC leads with: '2017 will be worse in every aspect of information security'
This report, which was focused on Africa, also predicts more consolidating and outsourcing of security – which seems likely in other parts of the world as well.

17) IBM – The twelve predictions offered by IBM were a mix of industry experts and their own internal security leaders in various industries. They lead with more adoption of

intelligence-led approaches to threats. Full disclosure: I am one of the experts included in the IBM list, with one of my predictions regarding fake news and online deception.
And for a few added extra predictions to check out, Dark Reading offers eight bold security predictions, including the LogRhythm prediction from CISO James Carder that the entire Internet will go down for a day. Also on the list – Tripwire's prediction that 2017 will bring the return of the worm.
I also like Microsoft's blog describing 17 women with predictions for 2017 and also for 2027.
Other good security prediction write-ups that I've seen include: Forbes.com, Betanews, The Register (UK), CIO.com on hiring, Computerworld, RSA, ITWorldCanada, Gigamon CTO Shehzad Merchant, ESET and Above Security.

2017 Prediction Wrap-Up

Almost everyone is saying that things will get worse in cyberspace before they get better. Most also think we are years away from meaningful, lasting cybersecurity answers. Still, our security industry progress is measured in small victories in many subcategories.
(As a side note, I have decided to cut back on the cyber prediction awards this year, offering only a few closing perspectives and trends regarding industry predictions.)
And yet, here are a few (see details earlier in article):
Most Creative — Watchguard Technology's 'Ransomworm'
Most Scary — LogRhythm prediction from CSIO James Carder that the entire Internet will go down for a day.
Most Common and Likely — More Internet of Things (IoT) Malware leading to more DDoS attacks. (It's already happening.)
Most Dull (yet also insightful) — Dan Lacey, White Hat Security: *'Nothing will change.'*
There is no doubt that the most common security predictions include an increase and expansion of cyberthreats against the cloud, more IoT attacks leading to disruptions, more (and different) ransomware and an increase in nation-state/cyberwar issues cutting across international lines.
What's missing? Companies have again held back on predicting a major Cyber Pearl Harbor or Cyber 9/11 type event, but many did predict that cyberterrorism will be growing more destructive in 2017. There is also a lack of government cybersecurity predictions covering what the new Trump Administration might do in the coming year. Finally, I was surprised that we didn't see more of a spotlight on 'bug bounties' or coordinated vulnerability disclosure programs - which I think will surge in government and other industries in the next few years.
For a wider view on global security trends in 2017, I encourage readers to take a look at the 2017 Global Forecast from the Center for Strategic & International Studies (CSIS). This website offers many in-depth insights, along with a 107-page report that covers many security topics, including cybersecurity.
In conclusion, the cybersecurity market is growing rapidly. According to cybersecurityventures.com market report, "We anticipate 12-15 percent year-over-year growth through 2021. ...
The U.S. government has increased its annual cybersecurity budget by 35 percent, going from $14 billion budgeted in 2016 to $19 billion in 2017. This is a sign of the times and there's no end in sight. Incremental increases in cyber security spending are not enough. We expect businesses of all sizes and types, and governments globally, to double down on cyber protection."
So despite some less than encouraging predictions regarding online safety and security, the future looks bright in 2017 for those who can offer workable solutions to solve security problems in cyberspace.
As Thomas Edison reportedly said last century: "Opportunity is missed by most people because it is dressed in overalls and looks like work."
And, "There's a way to do it better — find it."

Attackers can make it impossible to dial 911

By Mordechai Guri, Yisroel Mirsky, and Yuval Elovici
Source: http://www.homelandsecuritynewswire.com/dr20170106-attackers-can-make-it-impossible-to-dial-911

Jan 06 – It's not often that any one of us needs to dial 911, but we know how important it is for it to work when one needs it. It is critical that 911 services always be available – both for the practicality of responding to emergencies, and to give people peace of mind. But a new type of attack has emerged that can knock out 911 access – our research explains how these attacks occur as a result of the system's vulnerabilities. We show these attacks can create extremely serious repercussions for public safety.

In recent years, people have become more aware of a type of cyberattack called "denial-of-service," in which websites are flooded with traffic – often generated by many computers hijacked by a hacker and acting in concert with each other. This happens all the time, and has affected traffic to financial institutions, entertainment companies, government agencies and even key internet routing services.

A similar attack is possible on 911 call centers. In October, what appears to be the first such attack launched from a smartphone happened in Arizona. An 18-year-old hacker was arrested on charges that he conducted a telephone denial-of-service attack on a local 911 service. If we are to prevent this from happening in more places, we need to understand how 911 systems work, and where the weaknesses lie, both in technology and policy.

Understanding denial of service

Computer networks have capacity limits – they can handle only so much traffic, so many connections, at one time. If they get overloaded, new connections can't get through. The same thing happens with phone lines – which are mostly computer network connections anyway.

So if an attacker can manage to tie up all the available connections with malicious traffic, no legitimate information – like regular people browsing a website, or calling 911 in a real emergency – can make it through.

This type of attack is most often done by spreading malware to a great many computers, infecting them so that they can be controlled remotely. Smartphones, which are after all just very small computers, can also be hijacked in this way. Then the attacker can tell them to inundate a particular site or phone number with traffic, effectively taking it offline.

Many internet companies have taken significant steps to guard against this sort of attack online. For example, Google Shield is a service that protect news sites from attacks by using Google's massive network of internet servers to filter out attacking traffic while allowing through only legitimate connections. Phone companies, however, have not taken similar action.

Addressing the 911 telephone system

Before 1968, American emergency services had local phone numbers. People had to dial specific numbers to reach the fire, police or ambulance services – or could dial "0" for the operator, who could connect them. But that was inconvenient, and dangerous – people couldn't remember the right number, or didn't know it because they were just visiting the area.

The 911 system was created to serve as a more universal and effective system. As it has developed over the years, a 911 caller is connected with a specialized call center – called a public safety answering point – that is responsible for getting information from the caller and dispatching the appropriate emergency services.

These call centers are located in communities across the country, and each provides service to specific geographic regions. Some serve individual cities, while others serve wider areas, such as counties. When telephone customers dial 911 on their landlines or mobile phones, the telephone companies' systems make the connection to the appropriate call center.

To better understand how denial-of-service attacks could affect 911 call systems, we created a detailed computer simulation of North Carolina's 911 infrastructure, and a general simulation of the entire U.S. emergency-call system.

Investigating the impact of an attack

After we set up our simulation, we attacked it to find out how vulnerable it is. We found that it was possible to significantly reduce the availability of 911 service with only 6,000 infected mobile phones – just

0.0006 percent of the state's population.

Using only that relatively small number of phones, it is possible to effectively block 911 calls from 20 percent of North Carolina landline callers, and half of mobile customers. In our simulation, even people who called back four or five times would not be able to reach a 911 operator to get help.

Nationally, a similar percentage, representing just 200,000 hijacked smartphones, would have a similar effect. But this is, in a certain sense, an optimistic finding. Trey Forgety, the director of government affairs for the National Emergency Number Association, responded to our findings in the Washington Post, saying, "We actually believe that the vulnerability is in fact worse than [the researchers] have calculated."

Policy makes the threat worse

These sorts of attacks could, potentially, be made less effective if malicious calls were identified and blocked at the moment they were placed. Mobile phones have two different kinds of identifying information. The IMSI (International Mobile Subscriber Identity) is the phone number a person must call to reach that phone. The IMEI (International Mobile Station Equipment Identity) is used to track the specific physical device on the network.

A defense system could be set up to identify 911 calls coming from a particular phone that has made more than a certain number of 911 calls in a given period of time – say more than 10 calls in the last two minutes.

This raises ethical problems – what if there is a real and ongoing emergency, and someone keeps losing phone reception while talking to a dispatcher? If they called back too many times, would their cries for help be blocked? In any case, attackers who take over many phones could circumvent this sort of defense by telling their hijacked phones to call less frequently – and by having more individual phones make the calls.

But federal rules to ensure access to emergency services mean this issue might be moot anyway. A 1996 Federal Communications Commission order requires mobile phone companies to forward all 911 calls directly to emergency dispatchers. Cellphone companies are not allowed to check whether the phone the call is coming from has paid to have an active account in service. They cannot even check whether the phone has a SIM card in place. The FCC rule is simple: If anyone dials 911 on a mobile phone, they must be connected to an emergency call center.

The rule makes sense from a public safety perspective: If someone is having (or witnessing) a life-threatening emergency, they shouldn't be barred from seeking help just because they didn't pay their cellphone bill, or don't happen to have an active account.

But the rule opens an vulnerability in the system, which attackers can exploit. A sophisticated attacker could infect a phone in a way that makes it dial 911 but report it does not have a SIM card. This "anonymized" phone reports no identity, no phone number and no information about who owns it. Neither the phone company nor the 911 call center could block this call without possibly blocking a legitimate call for help.

The countermeasures that exist, or are possible, today are difficult and highly flawed. Many of them involve blocking certain devices from calling 911, which carries the risk of preventing a legitimate call for help. But they indicate areas where further inquiry – and collaboration between researchers, telecommunications companies, regulators and emergency personnel – could yield useful breakthroughs.

For example, cellphones might be required to run a monitoring software to block themselves from making fraudulent 911 calls. Or 911 systems could examine identifying information of incoming calls and prioritize those made from phones that are not trying to mask themselves. We must find ways to safeguard the 911 system, which protects us all.

Mordechai Guri *is Head of R&D, Cyber Security Research Center; Chief Scientist, Morphisec endpoint security, Ben-Gurion University of the Negev.*

Yisroel Mirsky *is Ph.D. Candidate in Information Systems Engineering, Ben-Gurion University of the Negev.*

Yuval Elovici *is Professor of Information Systems Engineering, Ben-Gurion University of the Negev.*

France thwarts 24,000 cyber-attacks against defence targets

Source: http://www.bbc.com/news/world-europe-38546415

Jan 08 – **France says it was the subject of 24,000 cyber-attacks against defence targets last year.**

Defence Minister Jean-Yves Le Drian said such attacks were doubling every year and this year's presidential elections could be targeted.

He said it would be "naive" to think France was immune to the type of cyber-campaign that targeted the US election, which has been blamed on Russia.

Mr Le Drian is overseeing an overhaul of France's cyber-security operations.

Cyber-attacks in France have increased substantially in the last three years and have become a serious threat to the country's infrastructure, Mr Le Drian said.

In an interview with Le Journal du Dimanche newspaper, Mr Le Drian said that France "should not be naive". He said that thousands of external attacks had been blocked, including attempts at disrupting France's drone systems.

His warning comes in the wake of a US intelligence report alleging that Russia was involved in an attempt to influence the 2016 presidential campaign.

Russia denies any involvement in cyber-attacks or hacking.

French elections in April and May this year are being carefully watched after the surprise victory of US President-elect Donald Trump, who said on Saturday that those who oppose good relations with Russia are "stupid people, or fools".

French conservative candidate Francois Fillon has said that he wants to improve relations with Russia and has been praised by Russian president Vladimir Putin. Far-right candidate Marine Le Pen also favours closer relations with Russia.

Relations between the two countries deteriorated after France's socialist president, Francois Hollande, played a key role in imposing sanctions on Russia when Crimea was annexed by Russia in 2014.

Mr Hollande also suggested last year that Russia could face war crimes charges over its bombardment of the Syrian city of Aleppo.

In April 2015, a powerful cyber-attack came close to destroying French TV network TV5Monde, which was taken off air.

A group calling itself the Cyber Caliphate, linked to so-called Islamic State (IS), initially claimed responsibility. But an investigation later discovered that it was carried out by a group of Russian hackers.

London NHS hospital trust hit by cyber-attack

Source: https://www.theguardian.com/technology/2017/jan/13/london-nhs-hospital-trust-hit-by-email-cyber-attackers

Jan 13 – **The largest NHS trust in England has been hit by a cyber-attack that could affect thousands of files across at least four London hospitals.**

Barts health trust, which runs five hospitals in east London – the Royal London, St Bartholomew's, Whipps Cross, Mile End and Newham – has sent a message to staff urging them not to open email attachments from unknown senders.

"We are urgently investigating this matter and have taken a number of drives offline as a precautionary measure, a Barts spokeswoman said. "We have tried and tested contingency plans in place and are making every effort to ensure that patient care will not be affected."

It was reported earlier on Friday that the trust had been targeted with **ransomware**, which is

normally delivered via emails that trick the recipient into opening attachments and releasing malware on to their system. But the spokeswoman ruled out such an attack on Friday night.

The trust has not said how much of its system has been affected by the attack or whether patient data has been compromised but it said it believed that most of the affected system was housing corporate data. The trust's filing system between departments has been turned off while the investigation takes place.

Staff at the Royal Free London foundation trust were also warned to beware of attacks on Friday, the Guardian has learned. "We have been informed of a major cyber-attack on NHS organisations. Please exercise extreme caution when opening any email attachments from unknown source or that don't seem relevant to you. We will be carrying out security scans on all computers within the trust so please leave them switched on until further notice," wrote the trust's IT director, Tosh Mondal.

A spokesman said the email was in reaction to the Barts attack and that the Royal Free London, as well as Barnet and Chase Farm hospitals, had not been affected.

NHS Digital said it was aware that Barts had been infected by a "virus which has affected their IT systems".

A spokesperson said: "This issue highlights the fact that there are threats to data security within the health and care sector, as with any other sector. We remain committed to supporting the protection of data with the highest possible security standards, high levels of security expertise from the centre and appropriate training and awareness of the risks for all staff."

She declined to answer questions about whether other NHS trusts had been affected, how much data may have been affected and who may be behind the attack.

In October, the Northern Lincolnshire and Goole foundation trust was hit by an attack in which malware was used to encrypt files and **demand a ransom** in order to restore access. The trust did not pay the ransom but was forced to cancel patient appointments as its systems were shut down to remove the virus.

John Bambenek, a threat intelligence manager at the firm Fidelis Cybersecurity, said: "The trouble is that local authorities and governments aren't very prepared and they have extremely valuable information that simply can't be lost, so they're a tempting target for cybercriminals.

"Cyber defence is essential, but it's no longer enough; organisations of all sizes need to invest in detecting threats as well. Only then will cyber criminals be caught early enough to expel them from the network before serious damage is done."

Devastating wildfires in Eastern forests likely to be repeated

Source: http://www.homelandsecuritynewswire.com/dr20161227-devastating-wildfires-in-eastern-forests-likely-to-be-repeated

Dec 27 – **The intense wildfires that swept through the Smoky Mountains in Tennessee late last month were a tragic melding of the past and the future,** according to a researcher in Penn State's College of Agricultural Sciences.

And the fast-moving, wind-whipped blazes that burned more than 150,000 acres, killed fourteen people and damaged 2,400 structures in Gatlinburg and Sevier County may be a portent of things to come, he warned.

"Many people have been lulled into believing that it is just the West that is prone to devastating wildfires, but that's not true," said Marc Abrams, professor of forest ecology and physiology, who for three decades has studied the historic role of fire in Eastern forests.

"Fire has played an important role historically in the forest ecosystem in the eastern United States, but the balance created by frequent — but not catastrophic — forest fires was upset by the Smokey Bear fire suppression regimen beginning in the late 1940s. Now, Eastern forests, when faced with prolonged drought, are more vulnerable to hotter-burning, terribly destructive wildfires."

Penn State notes that Abrams has published a series of research papers that focused on how Native Americans used fire to manage Eastern forests and made the forests more productive in yielding foods for themselves and the wildlife on which they depended. He believes the absence of fire has set the stage for catastrophic infernos such as those that recently raged through Tennessee.

Worse, Abrams sees a unique confluence between the past, when frequent forest fires were interrupted by a period of almost none, and the future, when a changing climate may well result in more severe and more prolonged droughts — resulting in fires more destructive than ever before.

"The fires we saw a few weeks ago in Tennessee were the worst in Eastern forests in my lifetime. The size of the area burned exceeded the number of acres that would burn in a normal year in the East," he said. "It's a reminder that the Eastern forests have always burned and are still pyrogenic, and because they are not managed with fire, they are now prone to have more catastrophic fires. The buildup of fuels is certainly a factor."

The southeastern United States is in a decades-long drought, Abrams pointed out, and he noted that some climate change models suggest extremely dry weather trends will continue. If so, more devastating fires like the recent Tennessee blazes are likely to occur. Although most climate change models suggest the East will, overall, receive slightly more precipitation, they also predict that more prolonged and more severe droughts will develop in places.

"We are seeing this in the Southeast and also in the Great Lakes states. Even though average precipitation has slightly increased, there are also areas in the East where drought has increased. It sounds counterintuitive, but it is occurring," he said.

"We have very pyrogenic forest vegetation in the eastern United States. Most of it is not as flammable as we think about in the West, where there are catastrophic crown fires in conifer forests every year, but most of the eastern U.S. is dominated by oak, hickory and pine, and these are fire-adapted species that have burned over thousands of years as part of their normal ecology."

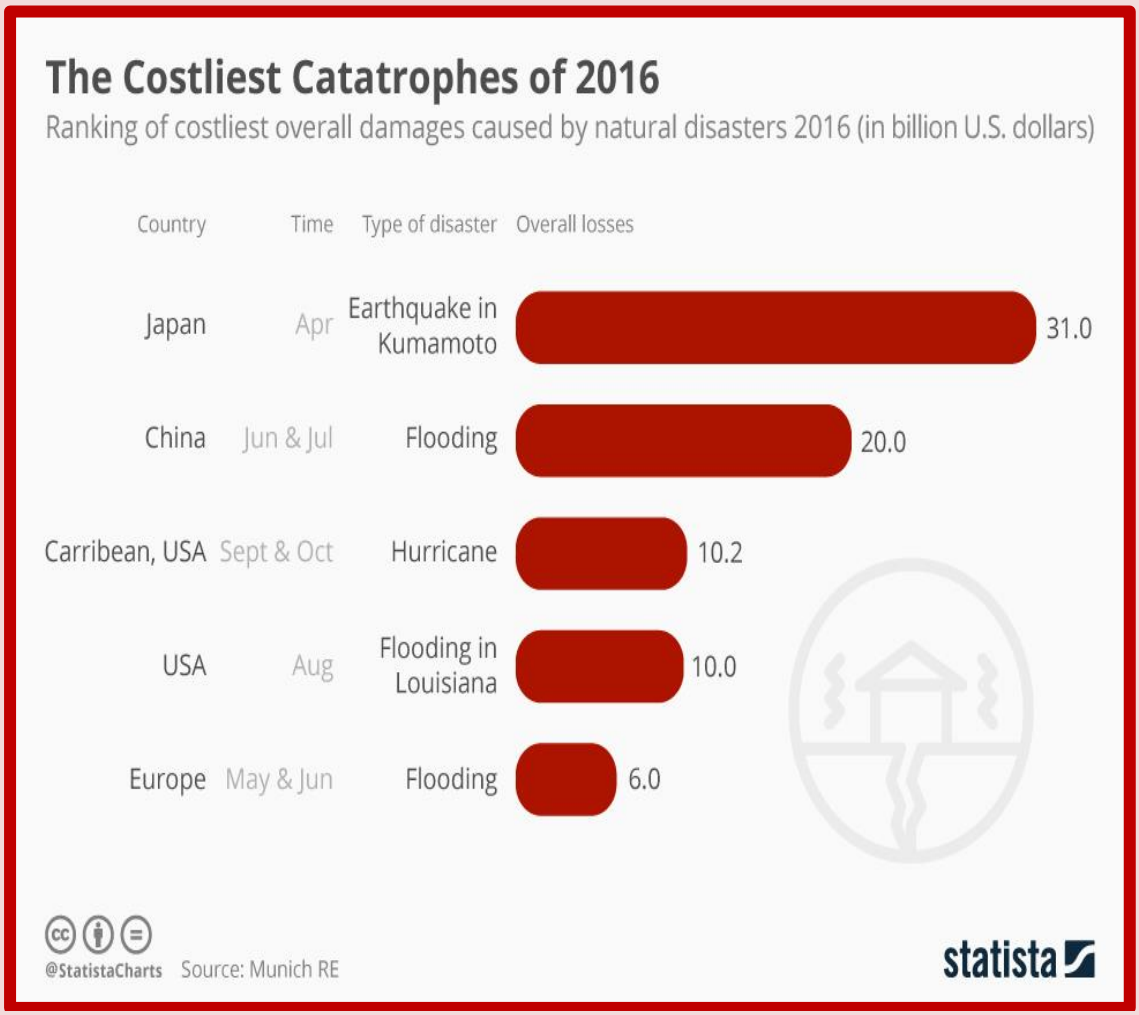
The melding of past and future for Eastern forests threatens to reverse a phenomenon that Abrams' research identified. In a paper published in January this year, he debunked claims that climate change has been the most important factor changing the composition of Eastern forests, presenting a

convincing argument that human activities such as land use and fire suppression have been more influential.

Everything that changed after the Europeans arrived in North America may be changing again as extreme droughts become more prevalent, Abrams contended.

A changing climate creating conditions conducive to devastating forest fires may become a primary driver of forest composition change. "Droughts have always occurred, but more severe, more persistent droughts have the potential to change forest composition most in the long run," he said.

"The long-term absence of fires in the East has caused a decrease in fire-adapted trees and an increase in species sensitive to fire and drought. This increased sensitivity will likely result in increased tree mortality associated with future fires and drought."



First RescueSim exam has been held and certified by IFV for Virtual Fire Fighting Examination

Source: www.vstepsimulation.com

Jan 09 – **Following the formal approval of the Dutch Safety Institute - Instituut Fysieke Veiligheid (IFV), the Dutch firefighting exam has been executed successfully for the first time using the RescueSim software.**

The thorough evaluation process started in 2015 with IFV's Bureau TEC, throughout the period RescueSim was furiously tested on suitability for the Virtual Firefighting Examination in compliance with the requirements of the IFV. VSTEP in cooperation with its customer H2K, specialised in fire service training programmes and industrial training courses, have jointly created several detailed and complex exam scenarios.

As a result, the RescueSim software has been accredited as virtual training software for usage for both

Incidentbestrijding Gevaarlijke Stoffen (IBGS; incident handling hazardous substances) and the Technische Hulpverlening (THV; incident involving technical assistance).
The first Virtual Fire Fighting Examination for Technische Hulpverlening using RescueSim took place on

the 13th of October 2016 at the premises of Veiligheidsregio Zaanstreek-Waterland. Six candidates were present to take the exam. The examination ended successfully with all six candidates passing their exams and the RescueSim software has proven to be a great support for the firefighting training.
Following this successful implementation, additional exams with RescueSim have been executed by Veiligheidsregio Zaanstreek-Waterland last month and new exams have been planned by H2K for this year.

Eric-Jan van Straten, Training and Exercises Co-operator, Veiligheidsregio Zaanstreek-Waterland: *"We have done examinations with RescueSim twice and both times we have had contact with VSTEP to make the scenarios as realistic as possible for*

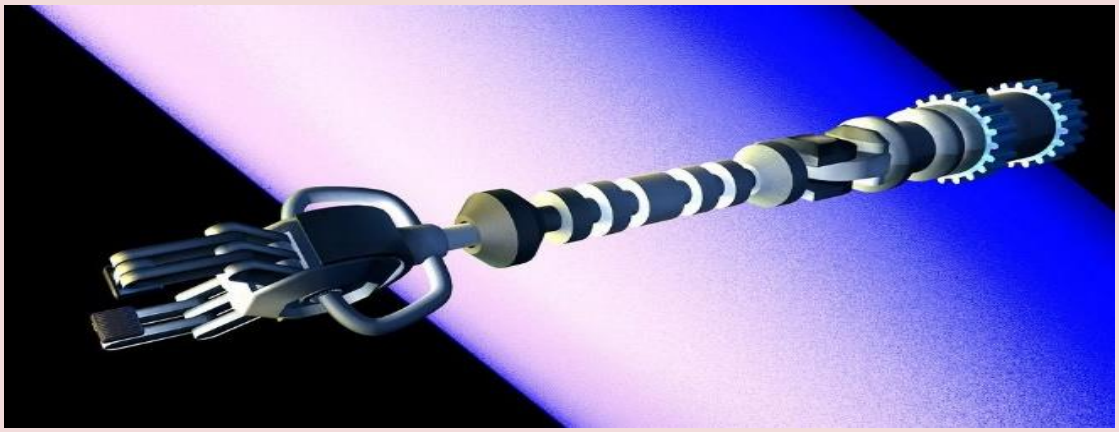
the exams. Both examinations were rounded successfully thanks to VSTEP's excellent support and now we have a reliable system with good scenarios to prepare our commanders for their official exams."

Ronald de Roos, Director, H2K: *"H2K has used RescueSim for its training courses since 2009 and we are extremely satisfied with this training system. The official certification of the RescueSim software, by the IFV, gives us the opportunity to use the virtual software also for organising virtual firefighting exams."*

Robot Arm Will Help Transfer Wounded Soldiers

Source: http://i-hls.com/2017/01/robot-arm-will-help-transfer-wounded-soldiers/

Jan 05 – **RE2 Robotics** has been contracted by the US Military to design an assistive manipulator arm, basically, a robot arm, to help speed-up the transfer of wounded Army soldiers.



According to army-technology.com, the company will design the low-risk, user-friendly system as part of the first phase of the Small Business Innovation Research (SBIR) programme, that encourages domestic small businesses to engage in Federal research and development with potential for commercialization.

The robot arm aims to provide a reliable transportation option for patients with severely reduced mobility.

RE2 Robotics president and CEO Jorgen Pedersen told the company's website: "This programme is about more than developing cutting edge assistive manipulation technology.

It is about empowering our service men and women who have suffered severe mobility limitations to regain a degree of transportation independence. This is one of the main reasons why RE2 Robotics is in business – to develop technologies that improve quality of life."

The new development is intended for the Applied Robotics for Installation and Base Operations (ARIBO) automated transport system pilot project. The ARIBO looks to provide automated, on-demand transportation to wounded soldiers travelling between the Warrior Transition Battalion barracks and the Womack Army Medical Center in North Carolina.

Using the ARIBO Assistive Arm, patients can be quickly transferred from a wheelchair onto the ARIBO vehicle and back to a wheelchair at the destination.

Based in the US, RE2 Robotics develops mobile robotic technologies that enable robot users to remotely interact with the world via ground, air or underwater solutions. The company produces interoperable robotic manipulator arms with human-like performance, intuitive human-robot interfaces, and advanced autonomy software for mobile robotics.

Whose Lives Should Be Saved? Researchers Ask the Public

By Sheri Fink

Source: https://www.nytimes.com/2016/08/22/us/whose-lives-should-be-saved-to-help-shape-policy-researchers-in-maryland-ask-the-public.html

Mary Jo D'Amico, a nurse at Memorial Medical Center in New Orleans, fanned a patient waiting in the hospital's parking garage for helicopter transport after Hurricane Katrina in 2005. Doctors had to make life-or-death decisions on which hurricane victims to treat. Credit Brad Loper/The Dallas Morning News, via Associated Press

Aug 2016 – In a church basement in a poor East Baltimore neighborhood, a Johns Hopkins doctor enlisted residents to help answer one of the most fraught questions in public health: When a surge of patients — from a disaster, disease outbreak or terrorist attack — overwhelms hospitals, how should you ration care? Whose lives should be saved first?

For the past several years, Dr. Lee Daugherty Biddison, a critical care physician at Johns Hopkins, and colleagues have led an unusual public debate around Maryland, from Zion Baptist Church in East Baltimore to a wellness center in wealthy Howard County to a hospital on the rural Eastern

Shore. Preparing to make recommendations for state officials that could serve as a national model, the researchers heard hundreds of citizens discuss whether a doctor could remove one patient from lifesaving equipment, like a ventilator, to make way for another who might have a better chance of recovering, or take age into consideration in setting priorities.

At that first public forum in 2012 in East Baltimore, Cierra Brown, a former Johns Hopkins Hospital custodian, said she favored a random approach like a lottery. "I don't think any of us should choose whether a person should live or die," she said.

Alex Brecht, a youth program developer sitting across from her, said he thought children should be favored over adults. "Just looking at them, seeing their smiles, they have so much potential," he said.

"Who's going to raise them?" asked Tiffany Jackson, another participant.

The effort is among the first times, Dr. Daugherty Biddison said, that a state has gathered informed public opinion on these questions before devising policy on them. "I don't want to be in a position of making these decisions without knowing what you think," she told the residents. "We as providers," she said, "don't want to make those decisions in isolation."

Rationing already occurs in delivering medical care in the United States, though some practices are little acknowledged. Committees struggle regularly over policies for allocating scarce organs for transplant.

During widespread drug shortages in recent years, doctors have sometimes chosen among cancer patients for proven chemotherapy regimens and among surgical patients for the most effective anesthetics. And doctors sometimes have to choose among patients who need treatment in intensive care units, which are often filled to capacity.

In emergencies, the choices can have immediate life-or-death consequences. After Hurricane Katrina in 2005, doctors made ad hoc decisions about which groups of patients to evacuate from hospitals when floodwaters rose, the power failed and heat climbed. At one medical center, many of the sickest, chosen to go last, died. During the H1N1 influenza pandemic in 2009, thousands of young people developed severe respiratory distress. For some of the most critical cases, doctors tried treatment on heart-lung bypass machines. Rationing took place because the costly and resource-intensive therapy, which doctors were not sure would help, was available in only about 120 hospitals.

Similar scenarios have developed in other countries, wealthy and poor. After the 2011 earthquake and nuclear disaster in Fukushima, Japan, some patients at nearby hospitals, including babies, were selected for flights to safety, while others languished for days as medical supplies dwindled. At one hospital, dozens of older patients were apparently abandoned, according to a report in The Lancet, and many died.

And during the 2014 Ebola epidemic in West Africa, when doctors and nurses could spend only so many minutes inside hot biohazard suits, they struggled with impossible choices over which patients to give care.

Dr. Daugherty Biddison, a vice chairwoman in the department of medicine at Johns Hopkins, said she had first encountered scarce medical resources while doing missionary work overseas. She realized that even Johns Hopkins Hospital, a 1,145-bed facility anchoring the $7.7 billion Johns Hopkins Medicine enterprise, would fail to meet demand in a severe pandemic. When asked to help draw up a plan, she said, she felt uncomfortable with health professionals' making life-or-death judgments without knowing the values of the broader public.

At least 18 states from New York to California, and numerous hospitals, including the 152 medical centers operated by the Department of Veterans Affairs, have already developed protocols. Some efforts, including Maryland's, have received funding from a federal program supporting hospital preparedness. But relatively few people know about the plans for allocating scarce resources, and fewer still have been consulted.

Some of these guidelines are nuanced and flexible to context. But others call for doctors to categorically refuse hospital admittance to older adults and those with certain existing medical conditions, such as kidney failure or advanced cancer, in a severe pandemic.

In Maryland, participants in the forums, designed with the help of Carnegie Mellon University's program for deliberative democracy, tended to favor saving the most lives or years of life by prioritizing people who were expected to survive

their current illness or live the longest after being treated. However, many also said that a lottery or first-come-first-served approach would be appropriate for patients who had roughly equal chances of benefiting.

"If you have one ventilator and five people who are good candidates, there's going to have to be a random sort of chance aspect to it," said Dr. Eric Toner, a senior associate at the UPMC Center for Health Security and one of the project's leaders.

Unexpected questions emerged in the discussions: Should an undocumented immigrant be eligible to get a ventilator? What about a drug or alcohol abuser, or a prisoner? After being told by a facilitator that discrimination would not be allowed, one participant asked whether using age, one of the principles under discussion, would not also be a form of discrimination.

Taking ventilators from patients who did not appear to be improving was "the single most contentious issue," Dr. Toner said. Maryland's attorney general released an opinion in December that lifesaving medical technology, including ventilators, could be removed from patients during a catastrophic emergency and reassigned to others who could potentially benefit more from them. Dr. Toner said it would be hard for any system to work without reallocation.

But at the forums, many expressed reservations. One woman said that she had been in a coma, on a ventilator, and that her family had been encouraged to turn it off and let her die. "Health care providers are not God," another said. "I've seen it firsthand where they thought one thing and the outcome was different."

To avoid rationing, a woman proposed a "Susan G. Komen for disaster preparedness," a reference to the ubiquitous fund-raising movement for a breast cancer cure. Some said they would voluntarily refuse a ventilator to save the lives of other people, such as children or family members. A man questioned whether doctors would even have the time in an emergency to engage in formal rationing. Some with lower incomes said that health care rationing was already occurring based on the ability to pay.

Translating all these ideas into recommendations for the state, most likely in mid-2017, will be challenging. The organizers said that despite the complexity, they were now in a better position to provide the guidelines.

"We have a much fuller appreciation of what the community wants," said Howard Gwon, the director of the office of emergency management at Johns Hopkins Hospital.

Charles Blattberg, a professor of political philosophy at the University of Montreal, said he worried that the effort could result in overly precise guidelines.

"The kind of judgment that's required to arrive at a good decision in these situations needs to be extremely sensitive to the context," he said. "It's not about just abandoning one lone doctor to their own devices to make it up on the spot, but we can't go the other extreme in thinking we have the solution to the puzzle already; just follow these instructions. That works for technical problems. These are moral, political problems."

Ruth Faden, the founder of Johns Hopkins's Berman Institute of Bioethics, which participated in the project, said she saw value in the exercise far beyond a pandemic.

"It's a novel and important attempt," she said, "to turn extremely complicated core ethical considerations into something people can make sense of and struggle with in ordinary language."

Sheri Fink *is a correspondent at The New York Times, where her and her colleagues' articles on the West Africa Ebola crisis were recognized with the 2015 Pulitzer Prize for international reporting, the George Polk Award for health reporting and the Overseas Press Club Hal Boyle Award.*

Groundwater resources around the world could be depleted by 2050s

Source: http://www.homelandsecuritynewswire.com/dr20161229-groundwater-resources-around-the-world-could-be-depleted-by-2050s

Dec 29 – **Human consumption could deplete groundwater in parts of India, southern Europe, and the United States in the coming decades,** according to new research presented at the 2016 American Geophysical Union Fall Meeting.

New modeling of the world's groundwater levels finds aquifers — the soil or porous rocks that hold groundwater — in the Upper Ganges Basin area of India, southern Spain, and Italy could be depleted between 2040 and 2060.

In the United States, aquifers in California's Central Valley, Tulare Basin, and southern San Joaquin Valley, could be depleted within the 2030s. Aquifers in the southern High Plains, which supply groundwater to parts of Texas, Oklahoma and New Mexico, could reach their limits between the 2050s and 2070s, according to the new research.

By 2050, as many as 1.8 billion people could live in areas where groundwater levels are fully or nearly depleted because of excessive pumping of groundwater for drinking and agriculture, according to Inge de Graaf, a hydrologist at the Colorado School of Mines in Golden, Colorado.

"While many aquifers remain productive, economically exploitable groundwater is already unattainable or will become so in the near future, especially in intensively irrigated areas in the drier regions of the world," said de Graaf.

Knowing the limits of groundwater resources is imperative, as billions of gallons of groundwater are used daily for agriculture and drinking water worldwide, said de Graaf.

Previous studies used satellite data to show that several of the world's largest aquifers were nearing depletion. But this method can't be used to measure aquifer depletion on a smaller, regional scale, according to de Graaf.

The AGU says that in the new research, de Graaf and colleagues from Utrecht University in the Netherlands used new data on aquifer structure, water withdrawals, and interactions between groundwater and surrounding water to simulate groundwater depletion and recovery on a regional scale.

The research team used their model to forecast when and where aquifers around the world may reach their limits, or when water levels drop below the reach of modern pumps. Limits were considered "exceeded" when groundwater levels dropped below the pumping threshold for two consecutive years.

The new study finds heavily irrigated regions in drier climates, such as the U.S. High Plains, the Indus and Ganges basins, and portions of Argentina and Australia, face the greatest threat of depletion.

Although the new study estimates the limits of global groundwater on a regional scale, scientists still lack complete data about aquifer structure and storage capacity to say exactly how much groundwater remains in individual aquifers, she said.

"We don't know how much water there is, how fast we're depleting aquifers, or how long we can use this resource before devastating effects take place, like drying up of wells or rivers," de Graaf said.

Natural catastrophe losses at their highest for four years

Source: http://www.homelandsecuritynewswire.com/dr20170113-natural-catastrophe-losses-at-their-highest-for-four-years

Jan 13 – A number of devastating earthquakes and powerful storms made 2016 the costliest twelve months for natural catastrophe losses in the last four years. Losses totaled US$ 175 billion, a good two-thirds more than in the previous year, and very nearly as high as the figure for 2012 ($ 180 billion). The share of uninsured losses – the so-called protection or insurance gap – remained substantial at around 70 percent. Almost 30 percent of the losses, some $ 50 billion, were insured.

"After three years of relatively low natural catastrophe (nat cat) losses, the figures for 2016 are back in the mid-range, where they are expected to be. Losses in a single year are obviously random and cannot be seen as a trend," said member of the Board of Management Torsten Jeworrek. "The high percentage of uninsured losses, especially in emerging markets and developing countries, remains a concern. Greater insurance density is important, as it helps to alleviate the financial consequences of a catastrophe for more people. With its risk knowledge, the insurance industry would in fact be able to bear a much greater portion of such unpredictable risks."

Munich Re says that key nat cat figures of 2016 include:

- Both overall losses and insured losses were above the inflation-adjusted average for the past ten years ($ 154 billion and 45.1 billion respectively).
- Taking very small events out of the equation, 750 relevant loss events such as earthquakes, storms, floods, droughts, and heatwaves were recorded in the Munich Re NatCatSERVICE database. That is significantly above the ten-year average of 590.
- Some 8,700 lives were sadly lost as a result of these natural catastrophes, far fewer at least than in 2015 (25,400), yet within the ten-year average (60,600). The past year was thus the year with the fewest fatalities (after 2014, with 8,050 fatalities) in thirty years (1986: 8,600).
- The high number of flood events, including river flooding and flash floods, was exceptional and accounted for 34 percent of overall losses, compared with an average of 21 percent over the past ten years.

Earthquake in Japan most expensive natural catastrophe of 2016

The costliest natural catastrophes of the year occurred in Asia. There were two earthquakes on the southern Japanese island of Kyushu close to the city of Kumamoto in April (overall losses $ 31 billion; proportion of insured losses just under 20 percent), and devastating floods in China in June and July (overall losses $ 20 billion; only some 2 percent of which were insured).

North America was hit by more loss occurrences in 2016 than in any other year since 1980, with 160 events recorded. The year's most serious event here was Hurricane Matthew. Its greatest impact was in the Caribbean island nation of Haiti, which was still struggling to recover from the 2010 earthquake. Matthew killed around 550 people in Haiti, and also caused serious damage on the east coast of the United States. Overall losses totaled $ 10.2 billion, with over a third of this figure insured.

Series of storms in Europe, wildfires in Canada

North America was also impacted by other extreme weather hazards, including wildfires in the Canadian town of Fort McMurray in May, and major floods in the southern U.S. states in summer. In Canada, the mild winter with less snow than usual, and the spring heatwaves and droughts which followed, were the principal causes of the devastating wildfires that hit the oil-sand-producing region of Alberta, generating overall losses of $ 4 billion. More than two-thirds of this figure was insured. In August, floods in Louisiana and other U.S. states following persistent rain triggered losses totaling $ 10 billion, around a quarter of which was insured.

There was a series of storms in Europe in late May and early June. Torrential rain triggered numerous flash floods, particularly in Germany, and there was major flooding on the River Seine in and around Paris. Overall losses totaled some $ 6 billion (approximately €5.4 billion), around half of which was insured.

"A look at the weather-related catastrophes of 2016 shows the potential effects of unchecked climate change. Of course, individual events themselves can never be attributed directly to climate change. But there are now many indications that certain events – such as persistent weather systems or storms bringing torrential rain and hail – are more likely to occur in certain regions as a result of climate change", explained Peter Höppe, Head of Munich Re's Geo Risks Research Unit.

Ground-breaking discovery for world food security

Source: http://www.homelandsecuritynewswire.com/dr20170113-groundbreaking-discovery-for-world-food-security

Jan 13 – A University of Queensland team has made a discovery that could help conquer the greatest threat to global food security – pests and diseases in plants.
Research leader Professor Neena Mitter said BioClay – an environmentally sustainable alternative to chemicals and pesticides – could be a game-changer for crop protection.
"In agriculture, the need for new control agents grows each year, driven by demand for greater production, the effects of climate change, community and regulatory demands, and toxicity and pesticide resistance," she said.
"Our disruptive research involves a spray of nano-sized degradable clay used to release double-stranded RNA, that protects plants from specific disease-causing pathogens."
UQ says that the research, by scientists from the Queensland Alliance for Agriculture and Food Innovation (QAAFI) and UQ's Australian Institute for Bioengineering and Nanotechnology (AIBN) is published in Nature Plants.
Professor Mitter said the technology reduced the use of pesticides without altering the genome of the plants.
"Once BioClay is applied, the plant 'thinks' it is being attacked by a disease or pest insect and responds by protecting itself from the targeted pest or disease.
"A single spray of BioClay protects the plant and then degrades, reducing the risk to the environment or human health."
She said BioClay met consumer demands for sustainable crop protection and residue-free produce.
"The cleaner approach will value-add to the food and agri-business industry, contributing to global food security and to a cleaner, greener image of Queensland."
AIBN's Professor Zhiping Xu said BioClay combined nanotechnology and biotechnology.
"It will produce huge benefits for agriculture in the next several decades, and the applications will expand into a much wider field of primary agricultural production," Professor Xu said.

— Read more in Neena Mitter et al., "Clay nanosheets for topical delivery of RNAi for sustained protection against plant viruses," Nature Plants 3, Article number: 16207 (9 January 2017)

Six cosmic catastrophes that could wipe out life on Earth

By Daniel Brown

Source: http://www.homelandsecuritynewswire.com/dr20170119-six-cosmic-catastrophes-that-could-wipe-out-life-on-earth

Jan 19 – **If you ask yourself what the biggest threat to human existence is you'd probably think of nuclear war, global warming, or a large-scale pandemic disease. But assuming we can overcome such challenges, are we really safe?**
Living on our blue little planet seems safe until you are aware of what lurks in space. The following cosmic disasters are just a few ways humanity could be severely endangered or even wiped out. Happy reading!

1. High energy solar flare

Our sun is not as peaceful a star as one might initially think. It creates strong magnetic fields that generate impressive sun spots, sometimes many times larger than Earth. It also ejects a stream of particles and radiation – the solar wind. If kept in check by Earth's magnetic field, this wind can cause beautiful northern and southern lights. But when it becomes stronger, it can also influence radio communication or cause power outages.
The most powerful magnetic solar storm documented hit Earth in 1859. The incident, called the Carrington Event, caused huge interference with rather small scale electronic equipment. Such events must have happened several times in

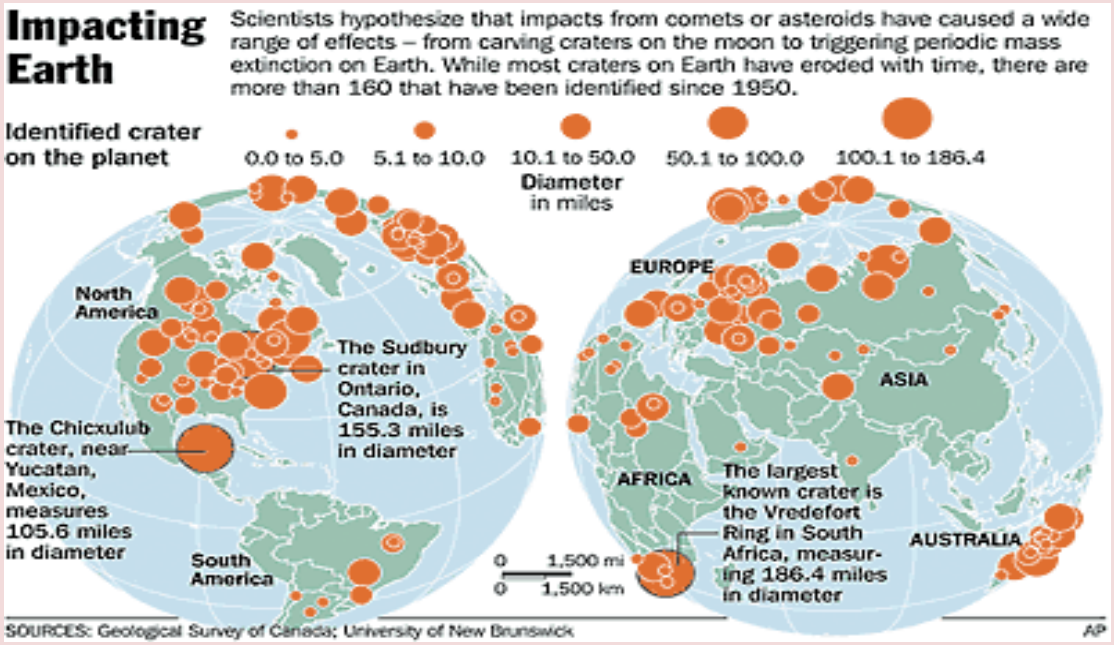
the past, too, with humans surviving.

But only in recent years have we become entirely dependent on electronic equipment. The truth is we would suffer greatly if we underestimate the dangers of a possible Carrington or even more powerful event. Even though this would not wipe out humanity instantly, it would represent an immense challenge. There would be no electricity, heating, air conditioning, GPS or internet – food and medicines would go bad.

2. Asteroid impact

We are now well aware of the dangers asteroids could pose to humanity – they are, after all, thought to have contributed to the extinction of the dinosaurs. Recent research has made us aware of the large host of space rocks in our solar system that could pose danger.

We are at the starting point of envisaging and developing systems for protecting us against some of the smaller asteroids that could strike us. But against the bigger and rarer ones we are quite helpless. While they would not always destroy Earth or even make it uninhabitable, they could wipe out humanity by causing enormous tsunamis, fires and other natural disasters.



3. Expanding sun

Where the previous cosmic dangers occur at the roll of a dice with a given probability, we know for certain that our sun will end its life in 7.72 billion years. At this point, it will throw off its outer atmosphere to form a planetary nebula, ending up as a stellar remnant know as a "white dwarf".

But humanity will not experience these final stages. As the sun becomes older, it will become cooler and larger. By the time it becomes a stellar giant it will be big enough to engulf both Mercury and Venus. Earth might seem safe at this point, but the sun will also create an extremely strong solar wind that will slow down the Earth. As a result, in about 7.59 billion years, our planet will spiral into the outer layers of the hugely expanded dying star and melt away forever.

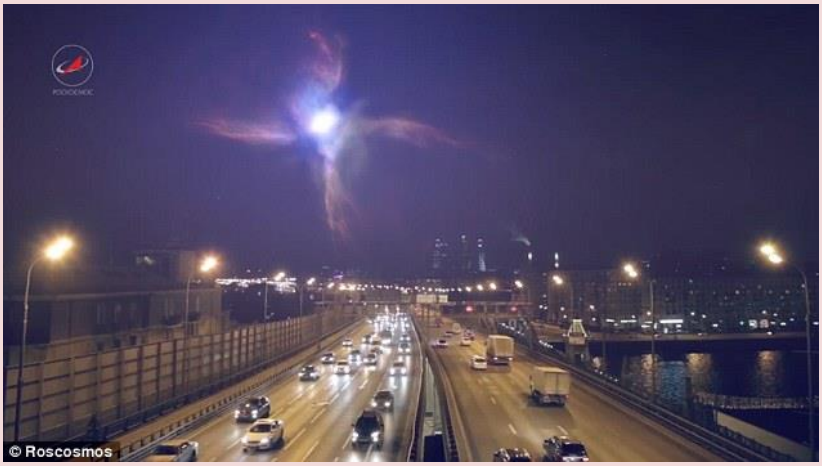
4. Local gamma ray burst

Extremely powerful outbursts of energy called gamma ray bursts can be caused by binary star systems (two stars orbiting a common centre) and supernovas (exploding stars). These energy bursts are extremely powerful because they focus their energy into a narrow beam lasting no longer than seconds or minutes. The resulting radiation from one could damage and destroy our ozone layer, leaving life vulnerable to the sun's harsh UV radiation.

Astronomers have discovered a star system – WR 104 – that could host such an event. WR 104 is about 5,200-7,500 light years away, which is not far enough to be safe. And we can only guess when the burst will happen. Luckily, there is the possibility that the beam could miss us entirely when it does.

5. Nearby supernovas

Supernova explosions, which take place when a star has reached the end of its life, occur on average once or twice every 100 years in our Milky Way. They are more likely to occur closer



to the dense centre of the Milky Way and we are about two-thirds of the way from the middle – not too bad.

So can we expect a nearby supernova anytime soon? The star Betelgeuse – a red super giant nearing the end of its life – in the constellation of Orion is just 460-650 light years away. It could become a supernova now or in the next million years. Luckily, astronomers have estimated that a supernova would need to be within at least 50 light years of us for its radiation to damage our ozone layer. So it seems this particular star shouldn't be too much of a concern.

6. Moving stars

Meanwhile, a wandering star on its path through the Milky Way might come so close to our sun that it would interact with the rocky "Oort cloud" at the edge of the solar system, which is the source of our comets. This might lead to an increased chance of a huge comet hurtling to Earth. Another roll of the dice.

The sun itself follows a path through the Milky Way that takes us through more or less dense patches of interstellar gas. Currently we are within a less dense bubble created by a supernova. The sun's wind and solar magnetic field help create a bubble-like region surrounding our solar system – the heliosphere – which shields us from interacting with the interstellar medium. When we leave this region in 20,000 to 50,000 years (depending on current observations and models), our heliosphere could be less effective, exposing Earth. We would possibly encounter increased climate change making life more challenging for humanity – if not impossible.

And life goes on…

The end of humanity on Earth is a given. But this is not something to make us crawl under a table. It is something that we cannot change, similar to our lives having a definite start and end. This is what defines us and makes us realise that the only thing we can do is make the most of our time on Earth. Especially when we know that Earth needs a careful balance to sustain humanity.

All the above scenarios harbour possible destruction, but in every instance they also offer beauty and wonder. In many cases, they produce what allowed us to be created. So rather than looking into the night sky and wondering what will kill us next, we should marvel at the depth of space, the wonders therein and the sublime nature of the universe. Be inspired by space. It offers future and meaning.

***Daniel Brown** is Lecturer in Astronomy, Nottingham Trent University.*