**Risk Mitigation Consulting Inc.**

*Intelligence and Analysis Division*

# OPEN SOURCE UPDATE

## 25 September 2017

## Threats

## Hazards

## Threats

## 'Bucket Bomb' Strikes London's Vulnerable Underground – *Terrorism*

**Excerpt:** Britain was hit by a terrorist attack on Friday morning, when a crude device exploded on a crowded London Underground train. Passengers described seeing a wall of fire.

The bomb, wrapped in a plastic grocery bag concealed in a bucket, exploded at 8:20 a.m. Friday at the height of the morning rush. The explosion and panic left 29 people injured, but none were killed.

It was the fifth terrorist attack in Britain this year and the first to hit London at its most vulnerable point — mass transit — since the 2005 bombings that killed 52.

The Islamic State asserted responsibility for the bucket bomb hours later in a message on its Amaq news site that said a "detachment" of its disciples had carried out the attack — language that suggested more than one assailant.

**Analyst Comment:** The latest IS-linked attack in London was the fifth terrorist attack of 2017 in the United Kingdom, and one of at least 14 IS-linked attacks since 2013 (per figures provided by the U.S. House Homeland Security Committee). The attack utilized a crude improvised explosive device (IED) that was placed on a train car during a peak Friday morning commute. The device only partially detonated, resulting in a fireball that injured several passengers on the train. 30 people were injured in the attack, including both the individuals who suffered burn injuries and some who suffered injuries as a result of the panic that ensued, although no deaths were reported.

The resulting manhunt has resulted in at least six arrests so far, although the investigation is ongoing. At least two of those arrested were refugees from Syria and Iraq, and one had previously been reported to a government anti-extremism office. Although the U.K. and other European countries maintain robust counterterrorism programs, attacks around Europe have continued at a steady pace. Per the U.S. House Homeland Security Committee, there have been at least 105 IS-linked incidents in Europe since 2013, including attack plots and attempts to provide financial or material support. The Islamic State continues to call for "lone wolf" sympathizers to carry out attacks against the West, and in some cases, has directed or aided such attacks. While it is currently unclear whether the latest London bombing was either IS-directed or IS-inspired, such attacks are likely to continue in Europe despite intense counterterrorism pressure.

*Source:* https://www.nytimes.com/2017/09/15/world/europe/uk-london-underground-tube-explosion.html?mcubz=1

# North Korea Fires Ballistic Missile Over Japanese Airspace Again –
## *Foreign Nation-State Military*

**Excerpt:** North Korea on Friday fired a ballistic missile that flew over Japanese airspace before crashing into the Pacific Ocean, South Korean and U.S. military officials said.

The ballistic missile was launched at 6:57 a.m. Friday Seoul time (5:57 p.m. Thursday ET) from the Sunan area of Pyongyang. It flew in an eastern direction around 2,300 miles and passed over Japanese airspace, a South Korean military official said.

The launch comes weeks after North Korea in late August fired a missile that traveled over Japanese airspace.

**Analyst Comment:** North Korea continues to conduct provocative missile tests in defiance of U.N. sanctions and overwhelming international pressure. The latest test was believed to be an intermediate-range ballistic missile which overflew the Japanese island of Hokkaido before landing in the Pacific Ocean. Another North Korean missile test also overflew Japanese territory just a few weeks prior. Both incidents prompted Japanese authorities to issue shelter-in-place orders, sparking fears among members of the public that an actual attack may be imminent as alert sirens blared.

Several international leaders have condemned North Korea's repeated ballistic missile tests, and rhetoric from the U.S. was markedly escalated. In a 19 September speech to the U.N. General Assembly, U.S. President Donald Trump vowed to "totally destroy" North Korea if the U.S. or its allies were attacked. On 21 September, North Korean leader Kim Jong Un issued a rare personal signed statement via the country's state-run news agency in which he stated that Trump would "pay dearly" for the remarks. On the same day, the North Korean foreign minister told reporters that retaliation could include "the…detonation of a [hydrogen bomb] in the Pacific."

*Source:* https://www.nbcnews.com/news/world/north-korea-possibly-preparing-intercontinental-ballistic-missile-test-n801401

## BlueBorne – *Cyber*

**Excerpt:** Armis Labs revealed a new attack vector endangering major mobile, desktop, and IoT operating systems, including Android, iOS, Windows, and Linux, and the devices using them. The new vector is dubbed "BlueBorne", as it spread through the air (airborne) and attacks devices via Bluetooth… BlueBorne allows attackers to take control of devices, access corporate data and networks, penetrate secure "air-gapped" networks, and spread malware laterally to adjacent devices. Armis reported these vulnerabilities to the responsible actors, and is working with them as patches are being identified and released.

The BlueBorne attack vector has several stages. First, the attacker locates active Bluetooth connections around him or her. Devices can be identified even if they are not set to "discoverable"

mode. Next, the attacker obtains the device's MAC address, which is a unique identifier of that specific device. By probing the device, the attacker can determine which operating system his victim is using, and adjust his exploit accordingly. The attacker will then exploit a vulnerability in the implementation of the Bluetooth protocol in the relevant platform and gain the access he needs to act on his malicious objective. At this stage, the attacker can choose to create a Man-in-The-Middle attack and control the device's communication, or take full control over the device and use it for a wide array of cybercriminal purposes.

**Analyst Comment:** BlueBorne poses a unique and potentially critical threat due to the medium by which it operates. Unlike the majority of attacks today, a BlueBorne attack spreads through the air, and is not reliant upon the internet. The user does not have to click on a link or download a questionable file. The attack does not require the targeted device to be paired to the attacker's device, or even to be set on discoverable mode, Bluetooth only needs to be active to expose the device to a potential attack. Since the Bluetooth process has high privileges on all operating systems, exploiting it provides virtually full control over the device.

Airborne attacks are particular contagious and spread quickly. Most common security measures (e.g. endpoint protection, mobile data management, firewalls, network security solution) are not designed to identify airborne threats, allowing existing security measures to be bypassed undetected. Airborne attacks are also effective when used upon secure internal networks which are "air gapped," meaning they are disconnected from any other network for protection, usually used by industrial systems, government agencies, and other critical infrastructure.

BlueBorne can serve any malicious objective, such as cyber espionage, data theft, ransomware, and even creating large botnets. A botnet is a number of Internet-connected devices, each of which is running one or more bots. Botnets can be used to perform distributed denial-of-service attack (DDoS attack), steal data, send spam, and allow the attacker access to the device and its connection. Since 2007, any Bluetooth vulnerabilities identified were of low severity. This is the first evidence of a significant security flaw via Bluetooth. Armis is "concerned that the vulnerabilities [they] found are only the tip of the iceberg, and that the distinct implementations of the protocol on other platforms may contain additional vulnerabilities."

At the time of the report, Armis claimed approximately 8.2 million Bluetooth-enabled devices were at risk. Since then, sources report that iPhones running iOS 10 are immune to the attack, and Microsoft deployed a patch to fix the bug in July. Google says it sent a fix to device manufacturers a month ago, but that patch must still be released by manufacturers.

*Source:* https://www.armis.com/blueborne/

## St. Louis Protest Activity – *Civil Disturbance*

**Excerpt:** Six years ago, former St. Louis Police officer Jason Stockley shot and killed Anthony Lamar Smith after a car chase in North St. Louis. Earlier this year prosecutors charged Stockley, who is white, with first-degree murder, alleging he planted a gun in Smith's car.

On Friday, Stockley was acquitted of the crime.

Immediately following the verdict protesters took to the streets in downtown St. Louis.

Like the protests that erupted in Ferguson following Michael Brown's shooting death at the hands of then-officer Darren Wilson, activists vow to protest throughout this weekend and into the coming weeks if necessary.

**Analyst Comment:** Local and state officials said they were prepared for potential unrest following the acquittal. Some schools in the St. Louis area were shuttered and events in the region were postponed as the verdict loomed. Concerts by U2 and Ed Sheeran were canceled last weekend amid security concerns. Immediately following the verdict, several hundred people gathered on Friday to peacefully protest the officer's acquittal.

Over the following weekend, a majority of the demonstrators were peaceful. However, after dark, smaller groups of agitators began to destroy property and assault police officers. Largely peaceful protests during the day have turned violent at night with some demonstrators carrying guns, bats and hammers, throwing water bottles, rocks and chairs, smashing windows and clashing with police. More than 160 people were arrested in protests over the weekend.

Saturday evening saw approximately 1,000 protesters gather at the mayor's home, throwing rocks and breaking windows. They were met by about 200 police in riot gear who tried to disperse them with tear gas. Overnight Sunday, police arrested more than 80 people after a peaceful protest turned violent as night fell. In a concentrated area downtown, some protesters smashed windows and overturned trash cans, while others threw chemicals and rocks at police, authorities said. The vast majority of protesters have been non-violent, with agitators only appearing in the evening in small groups to cause destruction.

Rallies this week have been largely peaceful. On Monday, about 100 protesters marched in silence along downtown streets Monday during the morning rush hour. On Wednesday, demonstrators blocked traffic near the St. Louis Galleria shopping mall. The protest broke up when police announced it had become an unlawful assembly. A protest has been planned for Thursday, and more events are expected to continue over the following days.

*Source:* http://www.npr.org/2017/09/15/551292324/protests-in-st-louis-after-ex-cop-acquitted-in-anthony-lamar-smith-murder-case

# Hazards

## Hurricane Recovery Health Effects – *Meteorological Hazards*

**Excerpt:** Emergency responders in the Everglades City area, a low-income fishing community walloped by Hurricane Irma last weekend, may be faced with a deadly public health crisis as families spend day after day in the mud, mold and water left behind by 10 feet of storm surge that destroyed hundreds of homes.

The deluge of potentially toxic storm water has raised the specter of widespread infection, sent at least half a dozen to the hospital, cost one man his leg and may have sickened another who died Saturday.

**Analyst Comment:** Following most natural disasters, the public health of effected communities will be extremely vulnerable. Access to sanitary drinking water, functional latrines, and appropriate nutrition are some of the most important factors in reducing the risk of contracting a communicable disease following a natural disaster.

Looking at the most recent areas recovering from hurricanes, standing water is a predominant concern. As homeowners spend hours a day cleaning and trying to salvage their homes, they may be working areas of remaining stagnant water or mud. These may be sources of potential infection, potentially containing sewage or toxins from local sources. Sewage water can crack skin on people's legs, creating open wounds at high risk of infection. Preexisting wounds can become infected. Even minor injuries sustained during clean-up efforts can turn deadly if exposed to standing water or mud. High heat and humidity, the current weather in recovering areas of Texas and Florida, also create ideal conditions for mold growth, irritating lungs and causing respiratory infections.

*Source:* https://www.usatoday.com/story/news/nation-now/2017/09/17/he-crying-and-moaning-agony-public-health-crisis-looms-after-irma/675822001/

## Hurricane Maria Leaves Puerto Rico Powerless, At Least 15 Dead in Dominica – *Meteorological Hazards*

**Excerpt:** Hurricane Maria regained major hurricane status early Thursday, strengthening to a Category 3 storm, as it left a devastated -- and completely powerless -- Puerto Rico in its wake and at least 15 dead people in Dominica.

The prime minister of Dominica, Roosevelt Skerrit, said at least 15 people died after the storm hit the island and 20 people were missing. Maria is also deemed responsible two deaths on Guadeloupe and one in Puerto Rico.

The strongest hurricane to hit Puerto Rico in more than 80 years left the entire island without electricity, making it difficult to assess just how much damage was caused by Maria's unrelenting onslaught.

**Analyst Comment:** Hurricane Maria became a named storm on 16 September, and reached hurricane status the next day. The storm rapidly intensified, reaching Category 5 on the Saffir-Simpson scale on 18 September. One day later, Maria made landfall on the island nation of Dominica as a Category 5 storm, before proceeding northwest toward Puerto Rico. On 20 September, Maria made landfall on Puerto Rico as a strong Category 4 storm, and is projected to take a northerly turn and not have any direct impacts on the continental U.S. Still, coastal effects are possible, and individuals in hurricane-prone areas should carefully monitor the storm.

Maria caused catastrophic damage among the islands of the Lesser Antilles and the Caribbean. In Dominica, 15 people were killed and at least 20 are considered missing, in addition to severe property damage and widespread communication disruptions. Maria also resulted in 2 deaths on the island of Guadeloupe. In Puerto Rico, Maria has resulted in at least 2 deaths. Puerto Rico also saw extensive property damage, particularly to the island's power grid. Puerto Rico's Governor, Ricardo Rosello, has stated that it may take several months to restore power to the island.

The 2017 Atlantic hurricane season has been highly active, with notable storms such as Hurricanes Harvey and Irma resulting in widespread property damage and a significant number of deaths. Prior to the 2017 season, on 25 May, the U.S. National Oceanic and Atmospheric Administration (NOAA), predicted a 70% chance of an above average season. Mid-season predictions trended upward, with NOAA notably raising their predicted number of storms and stating that the season had the potential to be extremely active (and could be the most active since 2010).

*Source:* http://www.foxnews.com/us/2017/09/21/hurricane-maria-regains-power-leaves-puerto-rico-powerless.html

# San Diego County Tackles Hepatitis A After Outbreak Kills 16 – *Biological Hazards*

**Excerpt:** An outbreak of hepatitis A has sickened 421 people and killed 16 in San Diego County between November and September, officials say. Additionally, 292 of the 421 have been hospitalized as a result of the viral infection, which causes inflammation of the liver.

Over the previous five years, the county recorded just 28 infections per year on average.

"This is an outbreak of unprecedented proportion, and we have not seen an outbreak of this nature as relates to hepatitis A before," said Dr. Wilma Wooten, public health officer and director of public health services for the county's Health and Human Services Agency.

Most of the infections, 65%, are occurring among people who are homeless, who use illicit drugs or who experience a combination of those two factors.

**7**

**Analyst Comment:** The recent hepatitis A outbreak in San Diego has largely affected the city's homeless population, illicit drug users, and those who have regular contact with members of the two groups (such as friends, healthcare workers, and social workers). San Diego has attempted to combat the spread of the virus through a multi-pronged approach including vaccination, education, and sanitation/hygiene efforts (such as bleaching public areas and providing hand-washing stations to the local homeless community). The outbreak has also spread to Los Angeles, where at least ten cases have been reported, of which two were locally-acquired and could not be traced to San Diego.

Per the World Health Organization (WHO, the hepatitis A virus is primarily spread when an uninfected (and unvaccinated) person ingests food or water that is contaminated with the feces of an infected person. The disease is closely associated with unsafe water or food, inadequate sanitation and poor personal hygiene. Unlike hepatitis B and C, hepatitis A infection does not cause chronic liver disease and is rarely fatal, but it can cause debilitating symptoms and fulminant hepatitis (acute liver failure), which is often fatal.

*Source:* http://www.cnn.com/2017/09/14/health/hepatitis-a-outbreak-san-diego-county/index.html