Risk Mitigation Consulting Inc.

Intelligence and Analysis Division

OPEN SOURCE UPDATE

September 2019

INTENT

This open source periodical is designed to provide an overview of relevant, publicly available information on threat and hazard events and analysis of potential impacts to the interests of the United States, both at home and abroad. This product is not intended to be a comprehensive overview of all threat and hazard news and inclusion in this product does not constitute a confirmation of credibility nor precedence by RMC.

Threats

Airline Mechanic Arrested for Sabotage Amid Labor Dispute – *Insider Threat*

Excerpt: American Airlines' nasty labor dispute with its mechanics escalated from major summer travel annoyance to scary situation Thursday [05 September] when a mechanic was arrested for allegedly trying to sabotage a July flight with 150 people on board.

Abdul-Majeed Marouf Ahmed Alani, a 60-year-old mechanic at American's Miami hub, was charged with "willfully damaging, destroying, disabling, or wrecking an aircraft" in a criminal complaint filed in U.S. District Court for the Southern District of Florida in Miami.

The tampering was discovered after American pilots got an error message as Flight 2834 from Miami to Nassau, Bahamas, was getting ready to depart on 17 July. They aborted takeoff, and the plane was taken out of service to be inspected.

Surveillance footage shows Alani at the gate before the flight and the complaint says he deliberately obstructed the ADM (air data module) system using a dark, Styrofoam-type material.

Analyst Comment: Fortunately, in this incident, a potential disaster was averted due to the attention of the pilots conducting routine pre-flight procedures. The air data module is a key component in airplane navigation systems which senses and computes key information regarding air pressure. Such information is utilized to indicate airspeed and is also used in autopilot systems. The absence of this information could make piloting an aircraft safely/accurately much more difficult and could potentially result in a crash.

The mechanic who sabotaged the air data module was arrested after being caught altering the system on video surveillance, and confessed to law enforcement that he was upset at a contract dispute between union employees and American Airlines which had affected him financially. He also clarified that he did not intend to cause damage, injury, or deaths, but rather sought to ground the plane in order to earn overtime pay. Still, this incident highlights the potential for insider threat incidents involving sabotage, as well as financial/work-related motives for conducting malicious acts.

Source: https://www.usatoday.com/story/travel/airline-news/2019/09/05/american-airlines-sabotage-mechanic-charged-disabling-system-labor-dispute/2228179001/

Arson Attack at Bar in Veracruz, Mexico – *Active Shooter/Active Assailant*

Excerpt: At least 27 people were killed in an attack in the Mexican state of Veracruz when assailants apparently locked the doors and emergency exits of the popular White Horse Nightclub and then set the building on fire.

The attack late Tuesday [27 August] came during a year of record violence for Mexico, which registered 14,603 homicides from January through June. The Mexican government under President Andrés Manuel López Obrador has struggled to piece together an effective security strategy as criminal organizations claim new ground, killing members of rival groups and civilians in the process.

Some early reports indicated the fire had been started with homemade bombs. López Obrador, in his morning news conference, said "the criminals went in, closed the doors, the emergency exits, and set fire to the place."

Analyst Comment: The attack comes amid growing violence in southern Veracruz state where the country's most powerful drug group, the Jalisco New Generation Cartel, has been battling another notorious group, the Zetas. The deadly attack came nearly eight years to the day after the Zetas drug cartel started a fire at a casino in the northern city of Monterrey, killing 52 people. Fractures within the Zetas are also likely to have contributed to the unrest. The governor of Veracruz said early evidence suggested the attack was motivated by efforts to sell drugs at the bar.

Other parts of Mexico have also seen dramatic incidents of cartel related violence in recent weeks. Events include the murder of several journalists, the stabbing of a priest, and the display of mutilated corpses, all within the last month. Homicides in Mexico rose 12% to 35,964 in 2018, or 29 per 100,000 inhabitants, according to the National Statistics Institute, and are up about 5% in the first seven months of this year.

In Veracruz, the state police force is significantly understaffed, an estimated 61% smaller than it should be. The state was supposed to receive 7,200 national guard members. However, most of the officers have been sent to assist in immigration enforcement, part of the U.S.-Mexico deal to reduce the number of migrants arriving at the U.S. border.

Source: https://www.washingtonpost.com/world/2019/08/28/arson-attack-bar-mexico-leaves-least-dead/

Israel Accused of Planting Spy Devices Near White House – *Foreign Intelligence Entities*

Excerpt: The U.S. government concluded within the past two years that Israel was most likely behind the placement of cellphone surveillance devices that were found near the White House and other sensitive locations around Washington, according to three former senior U.S. officials with knowledge of the matter.

But unlike most other occasions when flagrant incidents of foreign spying have been discovered on American soil, the Trump administration did not rebuke the Israeli government, and there were no consequences for Israel's behavior, one of the former officials said.

The miniature surveillance devices, colloquially known as "StingRays," mimic regular cell towers to fool cellphones into giving them their locations and identity information. Formally called

international mobile subscriber identity-catchers or IMSI-catchers, they also can capture the contents of calls and data use.

The devices were likely intended to spy on President Donald Trump, one of the former officials said, as well as his top aides and closest associates — though it's not clear whether the Israeli efforts were successful.

Analyst Comment: The discovery of the "Stingray" devices has been covered in a previous edition of the Open Source Update, although the origins of the devices was still unclear. Now, three former U.S. government officials told Politico that the devices (which are used to spy on cell phones) are believed to have been installed by individuals or groups acting on behalf of Israel. An Israeli Embassy spokesperson denied the allegations and many U.S. government agencies declined to comment, citing standard policies on matters related to intelligence and national security. Both President Trump and Israeli prime Minister Benjamin Netanyahu also downplayed allegations of spying.

The former officials quoted in Politico's report stated that the devices were attributed to Israel based on forensic analysis that entails examining the devices for unique information (such as specific manufacturers, parts, serial numbers, etc…) that would provide insight into the potential origin of such a device. The former officials indicated that such analysis is typically conducted by the FBI in coordination with other agencies, and that the analysis clearly pointed to Israel.

The "Stingray" devices were reportedly discovered in close vicinity to the White House (and other locations in Washington, D.C.), which may have provided a platform to eavesdrop on senior U.S. officials to include President Donald Trump, as well as Vice President Mike Pence, members of Congress, Cabinet Secretaries, Military/Intelligence leaders, and their aides/staff. While the discussion of classified information is prohibited on unsecured devices, it is possible that some sensitive information (or other information of intelligence value, such as potential blackmail opportunities) could be captured by monitoring the phones of individuals in senior government roles.

Source: https://www.politico.com/story/2019/09/12/israel-white-house-spying-devices-1491351

GAO: Energy Department Never Blacklists Risky Nuclear Tech Vendors – *Foreign Intelligence Entities*

Excerpt: The Energy Department is relying increasingly on foreign companies to build components for nuclear weapons, but it's never once used its authority to exclude risky tech vendors from the supply chain, according to a congressional watchdog.

In 2013, Congress authorized the energy secretary to prohibit vendors that "present a significant supply chain risk" from winning contracts related to the country's nuclear weapons programs. However, the Government Accountability Office found legal limitations and excessive

bureaucracy have kept officials from excluding any vendors for nearly six years, despite growing risks to the country's nuclear supply chain.

Those enhanced procurement authorities will likely continue to go unused unless Congress amends the law, leaving the door open for adversaries to "introduce into the components malicious code or malware that could … undermin[e] confidence in the nuclear weapons systems and their operational effectiveness," auditors said in a report.

Though the energy secretary makes the final decision to blacklist risky vendors, the National Nuclear Security Administration is responsible for determining when that authority should be used.

In 2018, NNSA officials told GAO there are multiple foreign tech companies that "present potential security vulnerabilities that could allow for unauthorized access to sensitive information." Still, they said they likely won't use enhanced procurement authorities to exclude those vendors because of multiple concerns with the statute.

Analyst Comment: The new GAO report indicates a serious security concern related to U.S. nuclear weapons systems. Foreign vendors who supply components used in nuclear weapons systems could potentially supply components for such systems that include malware, backdoors, surveillance tools, or other malicious capabilities. This remains a possibility because of bureaucratic roadblocks which has prevented blacklisting of risky vendors for at least the past six years. Foreign vendors may be subject to coercion or other influence from foreign nation-state governments, a concern which has been the basis for ongoing scrutiny of Chinese telecommunications firms Huawei and ZTE, as well as Russian cybersecurity firm Kaspersky Labs, among others. Supply chain security concerns have already resulted in recent policy changes at the Department of Defense, and it is likely that the Department of Energy will ultimately follow, although some security concerns may remain regarding existing systems.

Source: https://www.nextgov.com/cybersecurity/2019/08/energy-department-never-blacklists-risky-nuclear-tech-vendors-gao-says/159131/

DoS Cyberattack on U.S. Power Grid – *Cyber*

Excerpt: On 05 March 2019, an unprecedented Denial of Service (DoS) cyberattack occurred on American soil, targeted at the US power grid. This attack mainly affected the Western United States and was a fortunately low-impact attack. No blackouts were caused, and the machines in question were out of commission for no more than five minutes, according to the North American Electric Reliability Corp, or NERC.

Even so, this leaves a historical mark on American infrastructure, and clearly demonstrates the dangers of increased connectivity. A simple firewall vulnerability was enough to cause multiple devices to be compromised and rebooted from a single point of failure. While the impact this time around was minimal, this could have gone much worse.

Analyst Comment: The North American Electric Reliability Corp (NERC) released a report this month detailing the March cyberattack and the lesson learned from the event. According to the report, this attack exploited outdated firmware. A firmware fix to patch the vulnerability that was targeted had been released prior to the attack, but internal processes had been too lax to ensure that patch was applied in time to prevent this attack.

The U.S. power grid is increasingly reliant on digitalization and interconnectivity. To protect this critical infrastructure from cyberattacks, security measures must be consistently reexamined and improved. Improving the nation's cyber security will decreases the chances an attacker could gain control of an entire city's power grid or other utilities, potentially leading to the shutdown of a city and endangering lives in the process.

Once the patch was applied, the NERC continued to address the problem by implementing more safeguards in their networks. These steps included the following employing virtual private networks (VPNs), using fewer devices connected directly to the Internet, which reduces "attack surface" or potential points of failure and implementing access control lists (ACLs).

Source: https://hothardware.com/news/dos-us-power-grid

Hazards

Hurricane Dorian Impacts East Coast DoD Installations – *Meteorological Hazards*

Excerpt: Evacuations were ordered Thursday [05 September] for some Navy personnel in Virginia while residents at military bases in the Carolinas were asked to stay off roads and remain indoors as Hurricane Dorian continues to batter the East Coast with heavy rain and 50 mph winds.

More than 820 people, including families, guests, and Marines and Navy servicemembers, were evacuated from the Sandbridge area of Virginia Beach and Dam Neck Annex of Naval Air Station Oceana in advance of Dorian's arrival Friday [06 September], Navy Region Mid-Atlantic said.

"The safety of our personnel and their families remains our top priority as Hurricane Dorian approaches," said Rear Adm. Charles Rock, commander of Navy Region Mid-Atlantic. "For those traveling, please keep safety in mind and muster with your chain of command when reaching your safe haven. Roadways, interstates and highways may be congested as people travel out of harm's way."

Analyst Comment: Hurricane Dorian made landfall in the Bahamas as a powerful category 5 storm, causing widespread destruction and at least 50 deaths (although as of 13 September, 1,300 people remain listed missing). The storm then tracked toward the U.S. East Coast (albeit losing strength), to include several locations that host DoD installations. As a result, a number of precautions were taken, to include the evacuation of personnel, relocation of aircraft and naval vessels, and emergency preparations such as sandbagging in anticipation of flooding. However, impacts to the DoD from Dorian were relatively minor when compared to recent storms such as Hurricane Michael, which devastated Tyndall AFB in October 2018, and Hurricane Florence, which affected a number of DoD installations in the Carolinas one month prior in September 2018.

Source: https://www.stripes.com/news/us/navy-evacuates-some-personnel-in-virginia-ahead-of-dorian-other-east-coast-bases-assess-damage-1.597508

Extreme Wildfires Rage Around the World – *Meteorological Hazards*

Excerpt: In South America, the Amazon basin is ablaze. Halfway around the world in central Africa, vast stretches of savanna are going up in flame. Arctic regions in Siberia are burning at a historic pace.

While the Brazilian fires have grown into a full-blown international crisis, they represent only one of many significant areas where wildfires are currently burning around the world. Their increase in severity and spread to places where fires were rarely previously seen is raising fears that climate change is exacerbating the danger.

Hotter, drier temperatures "are going to continue promoting the potential for fire," said John Abatzoglou, an associate professor in the department of geography at the University of Idaho, describing the risk of "large, uncontainable fires globally" if warming trends continue.

Wildfires contribute to climate change because not only do they release carbon dioxide, a major greenhouse gas, into the atmosphere but they can also kill trees and vegetation that remove climate-warming emissions from the air.

Analyst Comment: This summer, a number of nations have faced more numerous and severe fires, to include both wildfires and deliberately started, man-made fires. Many of these fires, particularly across Europe, were exacerbated by the record-breaking heat of this summer. In addition to the damage caused to man-made structures, these fires have had spread smoke and soot into the air and water. Areas that have battled unusually extreme fires this year include Angola, the Canary Islands, Congo, Brazil, France, Greenland, Indonesia, Malaysia, Russia, Singapore, Spain, Turkey, and the United States.

Man-made fires have become more frequent as countries seek to clear land for farming or livestock. In southeast Asia, 71% of peat forests were lost between 1990 and 2015 to clear land for palm oil production. The smog from the peat fires caused a haze that may has cause thousands of premature deaths. In Brazil, land in the amazon area is being cleared for soybeans and cattle. Some fires are clearing of the previous season's crop, while others clear previously protect Amazonian forests.

Other locations like California, and sub-Saharan Africa, are home to ecosystems that reliably experience large wildfires. While wildfires are important for those ecosystems, when these fires coincide with dry seasons, droughts, or extreme heat, they become significantly larger and more damaging.

As noted in earlier Open Source Updates, Alaska, Canada, Greenland, and Siberia have experienced wildfires in unusual areas due to record temperatures and drier plants.

Source: https://www.nytimes.com/2019/08/28/climate/fire-amazon-africa-siberia-worldwide.html

Vaping-Related Lung Disease in the U.S. – *Biological Hazards*

Excerpt: U.S. health officials have narrowed their investigation of a mysterious lung disease that has killed at least six people to 380 "probable" and "confirmed" cases, the Centers for Disease Control and Prevention said Thursday [12 September].

Doctors suspect vaping as a possible cause of the illnesses, which are spread out over 36 states and the U.S. Virgin Islands. The CDC said it's homed in on the 380 likely or confirmed cases, instead of the more than 450 "possible" illnesses it was reviewing last week. It will no longer release data on cases that are less certain, the agency said.

At least six people have now died from the illness, which doctors say resembles lipoid pneumonia, a specific type of pneumonia that occurs when oil enters the lungs. The most recent death was a man in Kansas who was over 50 years old and had underlying health issues, officials said.

Many of the cases have occurred in young people who were otherwise healthy. Of the 53 patients studied in Illinois and Wisconsin, the median age was 19 years old, officials wrote in a New England Journal of Medicine report.

Analyst Comment: A new study in the New England Journal of Medicine examined six vaping-related cases. The illnesses were shown to be affecting a certain type of white blood cells called macrophages, which help protect the immune system. Usually, the presence of lipid-laden macrophages in the lungs is caused by lipoid pneumonia. Lipoid pneumonia usually results from accidentally inhaling liquid into the lungs. Cases of vaping related illnesses have reported symptoms similar to lipoid pneumonia, including shortness of breath, coughing, and chest pain.

Currently, the dominant theory among experts is that the lung ailments are linked to the inhalation of vitamin E acetate, a substance now being used by black-market dealers as a THC vape oil cutting agent. Oil samples studied by the FDA showed high levels of vitamin E acetate. However, not all of the samples tested contained vitamin E acetate. Additionally, while most of the patients studied used THC vapes, others said they hadn't, detracting from the theory that these cases are exclusively connected to black-market THC cartridges. It is generally agreed that it is too early in the investigation to point to a singular cause. Health officials have recommended avoiding the use of e-cigarettes and THC vaping products amid the outbreak.

Source: https://www.cnbc.com/2019/09/12/cdc-narrows-investigation-of-mysterious-vaping-related-lung-disease.html

Cargo Ship Capsizes in Georgia – *Accidental Events*

Excerpt: The ship, which is 656 feet long and weighs 71,000 tons, departed the Brunswick port bound for Baltimore about 1 a.m. Sunday [08 September]. There was soon a fire on board. About 2 a.m., emergency responders, including the Coast Guard, were notified that the ship had capsized in St. Simons Sound off the shore of St. Simons Island.

The Golden Ray had 24 people aboard — 23 crew members and a pilot — along with 4,200 vehicles. Twenty people were rescued quickly, but the other four could not immediately make their way off.

Rescue teams tapped on the ship's metal and eventually heard taps back, indicating the four trapped aboard were still alive. It took several hours Monday [09 September], but all four crew members were extracted. All were in remarkably good condition, the Coast Guard said.

Analyst Comment: Environmental impact should be limited, though it is too soon to determine the full impact of the event. The Coast Guard has used absorbent booms, retrieving fuel and oil.

As the ship is on its side, fuel now has the potential to escape from the fuel vents. Attempts at sealing the vents are in progress.

The investigation into the cause of the capsize is in progress. The Golden Ray was making a turn into the open ocean before it capsized, indicating shifting cargo or something else upset the ship's balance enough to make it fall onto its side. Another possibility is that an unsecured door enabled the ship to partially fill with water and become unstable.

The capsized ship has led to the closure of shipping lanes and the Port of Brunswick. Removing the 71,000-ton ship will take weeks if not months. Due to the ship's close proximity to the shore, shipping channels have been impacted, and future salvaging plans will likely have a significant impact on marine traffic in the area.

Source: https://www.ajc.com/news/coast-guard-removal-capsized-ship-off-georgia-coast-could-take-weeks-longer/O37YvUGxrwU3ZkIjWuIrNO/

Air Force Jet Accidentally Fires Rocket Near Tucson, AZ – *Accidental Events*

Excerpt: Air Force officials are investigating after an A-10C Thunderbolt II fighter jet on a training mission accidentally fired a rocket near Tucson. Officials at Davis-Monthan Air Force Base the M-156 rocket landed Thursday morning [05 September] in a remote desert wash near Mount Graham.

They say there were no injuries, damage or fires from the accidental launch of the white phosphorus projectile in the Jackal Military Operations Area, which is about 60 miles northeast of Tucson. White phosphorus is used by the military in various types of ammunition to produce smoke for concealing troop movement and to identify targets.

Analyst Comment: The A-10 Thunderbolt II aircraft is utilized by the U.S. Air Force in a ground-attack/close-air support role, with a design based around a 30mm rotary cannon, as well as the capability to mount additional weaponry on the wings. In the recent incident, an M-156 rocket was reportedly fired accidentally from an A-10 conducting training operations near Tucson, AZ. While the incident occurred in a designated military training area, Air Force officials said the area is not an authorized location for live-fire munitions releases. The accidental firing of the rocket reportedly did not result in any injuries, damage, or fires, however, such impacts could have been possible, with fires being a notable concern given high temperatures and dry conditions in the Arizona desert. Furthermore, it was still unclear whether crewmember error or a mechanical malfunction caused the rocket to fire, although an Air Force investigation is ongoing.

Source: https://www.cbsnews.com/news/fighter-jet-accidentally-fires-rocket-a-10c-thunderbolt-ii-fires-m-156-rocket-in-arizona/