Risk Mitigation Consulting Inc.

Intelligence and Analysis Division

OPEN SOURCE UPDATE

November 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

GOP Members Bring Cell Phones into Capitol SCIF – *Insider Threat*

Excerpt: Dozens of House Republicans on Wednesday [23 October] stormed the secure facility inside the Capitol where impeachment investigators have been deposing witnesses, forcing a delay to the proceedings on the heels of damning new revelations that could further imperil President Donald Trump.

GOP lawmakers who do not sit on the three committees leading the inquiry refused to leave the Sensitive Compartmented Information Facility (SCIF) in the basement of the Capitol, prompting a standoff with Democrats that led the House sergeant-at-arms to intervene.

After a five-hour stalemate, the Republicans left and Deputy Assistant Secretary of Defense Laura Cooper began her testimony behind closed doors.

According to people familiar with the matter, some Republican lawmakers brought their cellphones into the secure area — a significant violation of House rules. Another person said the room had to be fully swept for potential security breaches, and Democrats said the Republicans compromised national security by bringing electronics into a secure area.

Analyst Comment: The "storming" of the SCIF was primarily a political statement due to Republicans' apparent dissatisfaction with the Democrat-led impeachment investigation against President Donald Trump. However, several GOP lawmakers reportedly brought their cell phones into the SCIF, which is strictly prohibited. SCIFs (Sensitive Compartmented Information Facilities) are secure areas specially designed and certified to handle classified information. SCIFs include physical security measures as well as strict security policies (to include the prohibition of personal electronic devices) in order to protect the classified information that is handled inside.

While it is important to note that merely bringing one's cell phone into a SCIF is a security violation, there is no current evidence to suggest that classified information was compromised by the lawmakers' demonstration. Still, concerns remain due to the potential for cell phones to be compromised to include the installation of spyware by malicious actors. Observers have noted that lawmakers may be at particular risk for spyware and other malicious software due to their positions, the sensitive subjects they discuss on a regular basis, and their proximity to other high-ranking government and military officials.

Moreover, following such a breach, the SCIF's integrity must be reverified by the relevant authorities, which one former Congressional staffer described as a "time-consuming, technical process." This required process impacts Congress' ability to deal with sensitive/classified matters until the SCIF is deemed to be secure.

Source: https://www.politico.com/news/2019/10/23/impeachment-republicans-trump-055688

Gunmen Attack Mining Convoy in Burkina Faso – *Terrorism*

Excerpt: Gunmen attacked a convoy near a Canadian mining site in Burkina Faso, killing at least 37 people and wounding 60 others, the regional governor said late Wednesday [6 November].

Montreal-based Semafo said the bloodshed happened about 25 miles (40 kilometers) from its Boungou mine in Burkina Faso's Eastern region and involved five buses of employees who were being accompanied by a military escort.

Col. Saidou Sanou, the region's governor, gave the provisional casualty toll in a statement. The mining company said only that it was aware of "several fatalities and injuries."

"Boungou mine site remains secured and our operations are not affected," Semafo said in its statement. "We are actively working with all levels of authorities to ensure the ongoing safety and security of our employees, contractors and suppliers."

The area has become increasingly precarious for Semafo, which operates two gold mines in Burkina Faso. Last year, an employee and subcontractor were killed when a bus was targeted by bandits, according to Canadian Press. Later last year, five members of Burkina Faso's security forces were killed in an attack near the Boungou mine.

Analyst Comment: There was no immediate claim of responsibility, but Islamic extremists have staged dozens of attacks on churches, police stations, foreign businesses, and public officials across the north of Burkina Faso over the last few years. Furthermore, the high death toll and targeting of a foreign company's employees suggest that well-armed jihadists carried out the assault. Past attacks by Islamic extremists in Burkina Faso have specifically targeted foreigners.

While neighboring countries have been subject to attacks from Islamic extremists for many years, Burkina Faso experienced its first major extremist attack in 2015. It is believed that the extremists came from neighboring Mali. Since then, the country's security situation has rapidly deteriorated, becoming increasingly violent. This attack on the mining convoy is believed to have been the deadliest attack in Burkina Faso since the Islamic extremists became active in 2015.

Burkina Faso is seen as a gateway south into coastal West Africa, and regional leaders worry the extremists could move or spread into Togo and Benin. Because of this, five regional countries, along with a French operation, have tried to coordinate military action and root out the extremists. Their efforts do not appear to have impacted the situation.

Source: https://time.com/5720597/burkina-faso-mine-attack/

Colorado Man Arrested for Plot to Attack Synagogue – *Terrorism*

Excerpt: A man who repeatedly espoused anti-Semitic views has been arrested in a plot to bomb a historic Colorado synagogue, federal officials said Monday [04 November]. The co-conspirators

turned out to be undercover agents. Court documents say Richard Holzer was arrested Friday [01 November] in Pueblo just after the agents brought him what were supposedly two pipe bombs along with dynamite to blow up Temple Emanuel. In fact, the undercover agents had phony bombs incapable of causing damage, authorities said.

The agents said Holzer described the inert explosives as "absolutely gorgeous" and said they should go ahead with the attack overnight to avoid police. He had allegedly earlier made threatening comments about Pueblo's Jewish community and said he wanted to plot "something that tells them they are not welcome in this town," according to a criminal complaint filed in federal court.

Analyst Comment: Holzer was originally determined to be a potential threat after a tip regarding his social media activity was submitted to law enforcement. An investigation was opened, and a number of undercover FBI personnel ultimately coordinated with Holzer until an arrest could be made. Holzer faces federal hate crime charges and has been described by officials as a domestic terrorist.

Although Holzer's plot was fortunately uncovered and stopped by law enforcement, there have been at least two recent attacks on synagogues in roughly the past year. In April 2019, a gunman opened fire on the Chabad of Poway in Poway, California, killing one and injuring three others. Just six months prior, in October 2018, a gunman opened fire on the Tree of Life Synagogue in Pittsburgh, Pennsylvania, killing eleven and injuring 6 others. These attacks were both committed by individuals who espoused a broader racist/white supremacist ideology in addition to anti-Semitic views. The targeting of houses of worship (particularly synagogues and mosques) by far-right/racist/white supremacist extremists is likely to continue for the foreseeable future.

Source: https://www.cbsnews.com/news/synagogue-attack-pueblo-colorado-stopped-by-fbi-alleged-white-supremacist-arrested-today-2019-11-04/

Social Media App TikTok Under CFIUS Review – *FIE*

Excerpt: The United States government has opened a national security review of a Chinese company's acquisition of the American company that became TikTok, the hugely popular short-form video app, according to people briefed on the inquiry.

The Committee on Foreign Investment in the United States, a federal panel that reviews foreign acquisitions of American firms on national-security grounds, is now reviewing the two-year-old deal after lawmakers raised concerns about TikTok's growing influence in the United States, said the people, who spoke on the condition of anonymity because the investigation was confidential. One of the people said that the American government had evidence of the app sending data to China.

The move is the latest in a back and forth between the United States and China, which are enmeshed in a global competition for technological dominance that has begun to cleave the high-tech world in two and start what some analysts refer to as a new Cold War.

Analyst Comment: TikTok is a social media app that hosts short video clips relating to music, comedy, or other creative pursuits. The investigation into TikTok has arisen for a variety of reasons, to include complaints by prominent U.S. lawmakers to include Chuck Schumer, Tom Cotton, and Marco Rubio. These lawmakers and other observers have noted that TikTok could be used to spy on U.S. citizens or be used as a platform for foreign influence campaigns. Additionally, the app is popular among U.S. military personnel, heightening the aforementioned concerns somewhat.

While TikTok's parent company may not engage in these types of malicious activity on its own, as a Chinese-owned firm it could be compelled to do so by the Chinese government. (Note: for more information on security concerns associated with foreign hardware and software companies, please refer to RMC's Intelligence and Analysis Division White Paper from February 2019 which discusses the subject in greater detail)

Source: https://www.nytimes.com/2019/11/01/technology/tiktok-national-security-review.html

Equifax Used "Admin" as Username/Password for Portal Prior to Data Breach – *Cyber*

Excerpt: Equifax used the word "admin" as both password and username for a portal that contained sensitive information, according to a class action lawsuit filed in federal court in the Northern District of Georgia.

The ongoing lawsuit, filed after the breach, went viral on Twitter Friday [18 October] after Buzzfeed reporter Jane Lytvynenko came across the detail.

"Equifax employed the username 'admin' and the password 'admin' to protect a portal used to manage credit disputes, a password that 'is a surefire way to get hacked,'" the lawsuit reads.

The lawsuit also notes that Equifax admitted using unencrypted servers to store the sensitive personal information and had it as a public-facing website.

When Equifax, one of the three largest consumer credit reporting agencies, did encrypt data, the lawsuit alleges, "it left the keys to unlocking the encryption on the same public-facing servers, making it easy to remove the encryption from the data."

Analyst Comment: The class action lawsuit against Equifax revealed weak cybersecurity practices at the credit reporting agency, to include the use of "admin" as a username/password for a portal containing sensitive personal information. Weak and/or default credentials can be exploited by malicious cyber actors to gain access into systems, networks, and databases, so individuals (particularly IT administrators) should always utilize strong passwords. Moreover, Equifax failed to properly encrypt servers containing sensitive personal information.

Per the U.S. Federal Trade Commission, the Equifax data breach lasted from mid-May through July of 2017, with hackers compromising roughly 143 million Americans' personal information, in addition to individuals from countries such as the United Kingdom and Canada. The exposed individuals' personal information could potentially be utilized by malicious actors for purposes to include credit card fraud or identity theft.

Source: https://finance.yahoo.com/news/equifax-password-username-admin-lawsuit-201118316.html

Fentanyl Found in Counterfeit Prescription Pills – *Narcotics*

Excerpt: Mexican drug cartels are making "mass quantities" of fake prescription pills containing the synthetic opioid fentanyl with the intention of selling them to users throughout North America, the U.S. Drug Enforcement Administration (DEA) said on Monday [4 November].

Mexico's cartels have for years diversified into a wide variety of illicit activity, helped by porous domestic law enforcement agencies as well as long-standing trafficking routes into the United States, their biggest market.

Meanwhile, opioid deaths in the United States have soared over the last two decades, driving a wave of government-backed efforts to disrupt illegal distribution and treat addicts.

The DEA said that 27% of a sample of counterfeit pills tested in the United States during the first three months of this year contained potentially lethal doses of fentanyl.

Analyst Comment: Fentanyl and other highly potent synthetic opioids remain the primary driver behind the ongoing opioid crisis, with fentanyl involved in more deaths than any other illicit drug. Fentanyl analogues are the particularly dangerous drugs because they are man-made and cheap. Pills containing fentanyl and fentanyl-laced heroin cause thousands of deaths every year in the United States. A lethal dose of fentanyl is estimated to be about two milligrams but can vary based on an individual's body size, tolerance, amount of the previous usage and other factors.

Counterfeit pills have hidden dangers causing one in four users to die, according to DEA field testing. In 2016, the DEA published an intelligence brief titled *Counterfeit Prescription Pills Containing Fentanyls: A Global Threat*. In the report they note that the equipment and materials necessary to produce these counterfeit drugs are widely available online for a small initial investment, greatly reducing the barrier of entry into production. Since 2014, U.S. law enforcement agencies have been seizing a new form of fentanyl—counterfeit prescription opioid pills containing fentanyl. The counterfeit pills often closely resemble the authentic medications they were designed to mimic, and the presence of fentanyl is only detected upon laboratory analysis. In addition to being deadly to users, fentanyl poses a threat to law enforcement officials and first responders as a potentially lethal dose of fentanyl can be accidentally inhaled or absorbed through the skin.

Source: https://www.reuters.com/article/us-mexico-drugs-dea-idUSKBN1XF012

Hazards

"Arctic Blast" Brings Record-Breaking Cold to the U.S. – *Meteorological Hazards*

Excerpt: Record-breaking cold and snowfall is numbing many parts of the U.S. from the Great Plains to the East Coast and north through New England. By Wednesday [13 November] the cold snap is expected to spread farther south to the upper Texas coast in what is being described as an "arctic outbreak" by the National Weather Service.

The dead-of-winter temperatures come with roughly five weeks of fall remaining on the calendar.

"The arctic airmass that has settled into the Plains will continue to spread record cold temperatures south and eastward into the Ohio Valley and down into the southern Plains," according to the National Weather Service.

It adds: "Low temperatures in the teens and 20s will be common along much of the East Coast, the Ohio Valley, and down as far south as the upper Texas coast, making it feel like the middle of winter for these areas."

An estimated 300 cold-weather records are expected to be tied or broken by Wednesday [13 November]. The National Oceanic and Atmospheric Administration estimates 30% of the continental U.S. is covered by snow.

Analyst Comment: Aside from direct health impacts of wind chill, frostbite, and hypothermia, extreme cold events such as this arctic blast can have a range of secondary effects. Extremely cold temperatures can cause ground freezing problems, especially if there is little snow cover. Buried water pipes can burst causing massive ice problems and loss of water pressure in metropolitan areas. This can lead to further public health and safety problems.

Accompanying snow and ice impacts almost every mode of transportation. Diesel engines are stressed and, often fuel gels in extreme cold weather impacting trucking and rail traffic. Icy conditions in Kansas were said to have caused the death of an 8-year-old girl in a three-vehicle crash in Osage County. In Lansing, Michigan, a two-vehicle crash resulted in three deaths. In southwestern Michigan, a man died Tuesday [12 November] after getting trapped beneath machinery he was using to clear snow, officials said.

Rivers and lakes can freeze, stopping barge and ship traffic. Subsequent ice jams threaten bridges and can close major highways. Icing poses a major threat to air travel as ice can accrete on the plane's wings or engines, and increase drag on the plane and lead to engine failure. This can result in lengthy flight delays and cancellations. During this arctic blast, an American Eagle flight slid off the runway at O'Hare Airport during a storm. O'Hare and Midway international airports saw thousands of flights delayed or canceled because of the weather.

Source: https://www.npr.org/2019/11/12/778636602/arctic-blast-grips-parts-of-the-u-s-with-snow-and-record-breaking-cold

Historic Repeat Flooding in Venice, Italy – *Meteorological Hazards*

Excerpt: Venice was inundated by exceptionally high water levels on Friday [15 November] just days after the lagoon city suffered the worst flood in more than 50 years.

The central St. Mark's Square was submerged and closed to tourists, while shops and hotels were once more invaded by rising waters bringing fresh misery to the fragile city.

Local authorities said the high tide peaked at 154 cm (5.05 ft), slightly below expectations and significantly lower than the 187 cm level reached on Tuesday [12 November] — the second highest tide ever recorded in Venice.

The central St. Mark's Square was submerged and closed to tourists, while shops and hotels were once more invaded by rising waters bringing fresh misery to the fragile city.

The Italian government declared a state of emergency for Venice on Thursday [14 November], allocating 20 million euros ($22 million) to address the immediate damage. Mayor Luigi Brugnaro predicted on Friday the costs would be vastly higher.

Analyst Comment: In normal conditions, tides of 80-90cm are generally seen as high but manageable. However, on Tuesday the 12th, tides rose to 187 cm. More than 80% of the city was flooded. This was the highest level in more than 50 years, damaging monuments, shops and homes. Only once since official records began in 1923 has the tide been higher - hitting 194cm in 1966.

Venice is over 1,600 years old. Built on uncompacted sediment, the city itself is sinking. Additionally, the mean sea level is estimated to be more than 20 cm higher than it was a century ago and set to raise much further. Venice's Tide Office said that because of the combined effect of the sinking and the rising of the sea, the water is now 30 centimeters (12 inches) higher against the buildings than it was when record-keeping began in 1873.

This week's tides were, in part, a result of sirocco winds blowing from Africa and pushing water from the shallow Adriatic Sea into Venice, and a full moon. However, climate scientists note that tides over 1.4 meters have become much more frequent in the past two decades. Of the 20 tides over 1.4 meters recorded from 1936 through Tuesday the 12th, more than half have occurred since 2000.

In 2003 work began on a flood barrier designed to protect Venice from high tides. It was supposed to be working by 2011, but current estimates say that it is not expected to start working until the end of 2021. Though nearly completed, the project still has not been even partially tested, and some parts have already started to corrode. It remains to be seen if these barriers will mitigate the effects of a rising ocean and a sinking city.

Source: https://www.cnbc.com/2019/11/15/venice-hit-by-another-ferocious-high-tide-flooding-city.html

Pneumonic Plague in China – *Biological Hazards*

Excerpt: Two people in China have been diagnosed with pneumonic plague, local health authorities confirmed, prompting fears of a wider outbreak of the deadly infectious disease.

The Beijing municipal government said on its website Tuesday [12 November] that two people in the autonomous region of Inner Mongolia in northern China were diagnosed with pneumonic plague and doctors in Beijing confirmed the diagnosis shortly after. The two patients have received "proper treatment in relevant medical institution of Chaoyang District and relevant disease prevention and control measures have been taken."

The diagnosis marks the second time the plague has been detected in the region in recent months. In May, a Mongolian couple died from bubonic plague, the most common form of plague, after eating the raw kidney of a marmot as a local folk remedy, Agence France-Presse news agency reported earlier this year.

Analyst Comment: There are three types of plague: bubonic, septicemic, and pneumonic. Plague can be a very severe disease in people, particularly in its septicemic and pneumonic forms, with a case-fatality ratio of 30% - 100% if left untreated. All three are caused by the bacterium Yersinia pestis usually found in small mammals and their fleas. It is generally transmitted between animals, and sometimes people, by the infected fleas, though each type has additionally means of transmission.

Bubonic plague is mainly spread by infected fleas from small animals. After exposure, flu like symptoms develop. These include fever, headaches, and vomiting. Swollen and painful lymph nodes occur in the area closest to where the bacteria entered the skin. It may also result from exposure to the body fluids from a dead plague infected animal. Septicemic plague is a deadly blood infection. Septicemic plague can cause the blood to form small clots. Without treatment it is almost always fatal. This disease is caused mainly by the bite of an infected rodent or insect. In rare cases it can also enter the body through an opening in the skin or by cough from another infected human.

Pneumonic Plague is a severe lung infection. Symptoms including fever, headache, rapidly developing pneumonia, shortness of breath, chest pain, and cough begin. If left untreated, the pneumonic plague is always fatal. Pneumonic plague may develop from untreated bubonic or septicemic plague after it spreads to the lungs. According to the CDC, it is the most infectious form of the plague and is the only form that can spread from person to person.

Due to the ability of this plague to spread from person to person, Chinese residents fear a wider outbreak may occur, stemming from those who were in contact with the infected individuals. In 2014, a man died of the plague in northwestern Gansu province in China and sparked the

quarantine of 151 people. The 30,000 people living in Yumen, the town where the man died, were also prevented from leaving, with police at roadblocks placed on the town perimeter.

Source: https://www.usnews.com/news/health-news/articles/2019-11-13/two-people-in-china-diagnosed-with-the-plague