Risk Mitigation Consulting Inc.

Intelligence and Analysis Division

OPEN SOURCE UPDATE

4 April 2018

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

11 Sickened in HAZMAT Incident at JB Myer-Henderson Hall – *CBRNE*

Excerpt: Three Marines exposed to a suspicious substance after an envelope was opened at Joint Base Myer-Henderson Hall in Arlington have been released from the hospital as authorities continue to investigate the incident.

The envelope was opened on the Marine Corps side of the base about 3 p.m. on 27 February, a news release said. Eleven people were sickened. Three Marines were taken to a hospital for evaluation. They were released at 10 p.m.

Leah Rubalcaba, a spokeswoman for Fort Myer, said the building was cleared for reentry around 11 p.m. and normal operations had resumed. The FBI and the Naval Criminal Investigative Service continue to investigate, she said. No further details about the incident were available.

Analyst Comment: The suspicious package opened at JB Myer-Henderson Hall sickened 11 individuals, including 3 Marines who were taken to a local hospital. At this time, limited information surrounding the incident is available in media reporting. The substance in the envelope has also not yet been publicly identified, nor has a suspect or a motive. Although the event is currently referred to as a "HAZMAT incident", terrorism does not appear to have been ruled out, and the FBI and NCIS are leading the investigation. Moreover, previous CBRNE attacks have targeted U.S. government entities, to include the 2001 anthrax attacks which targeted members of Congress.

Additionally, on 12 February, an envelope containing a suspicious substance was sent to the home of Donald Trump Jr., which was opened by his wife, Vanessa. As a precaution, she and two others were taken to the hospital for evaluation. The package was later determined to have contained cornstarch. A Massachusetts man was arrested in the incident, which also included a number of additional threatening letters to political figures around the country.

Source: https://www.washingtonpost.com/local/public-safety/fbi-ncis-continue-investigation-myer-henderson-hall-hazmat-incident/2018/02/28/c678d092-1cac-11e8-9496-c89dc446c2d3_story.html?utm_term=.bb6c2b3cf78f

Former Russian Military Intelligence Officer Poisoned in England – *CBRNE*

Excerpt: European Union leaders have backed U.K.'s assessment that the nerve agent attack on a former Russian double agent was almost certainly carried out by Moscow, saying, "there is no plausible alternative explanation."

Speaking in Brussels, Dutch Prime Minister Mark Rutte said it was "highly likely Russia is responsible," for the attack on 66-year-old Sergei Skripal and his daughter, Yulia, 33, at a shopping mall in southern England on March 4.

Britain's Prime Minister Theresa May won the backing of 27 other EU leaders at a summit Thursday. The bloc called the attack a "grave challenge to our shared security" and announced that it was recalling its ambassador to Russia.

The poison involved in the attack has been identified as Novichok, a military-grade nerve agent that was developed in a top-secret laboratory in Moscow in the 1980s and would be extremely difficult or impossible to obtain elsewhere.

Analyst Comment: Skripal's poisoning, which Britain says was caused by use of the Soviet-era military-grade nerve agent Novichok, is the first known offensive use of a nerve toxin in Europe since World War Two. The name Novichok applies to a group of nerve agents developed by the Soviet Union in the 1970s and 1980s. Novichok's existence was revealed in the 1990s. As nerve agents, the Novichok agents belong to the class of organophosphate acetylcholinesterase inhibitors. These chemical compounds prevent the normal breakdown of the neurotransmitter acetylcholine. Acetylcholine concentrations then increase to cause involuntary contraction of all muscles. This then leads to respiratory and cardiac arrest and finally death from heart failure or suffocation.

A chemical attack has the potential to affect those targeted, first responders, and near-by bystanders, depending on the location and scope of the attack. 48 people were hospitalized in relation to the incident including a police officer who fell ill after attending the incident. Only Mr. Skripal and his daughter Yulia remain in hospital. Investigators have identified 131 people who have potentially been in contact with the nerve agent. None has shown symptoms.

Source: https://www.npr.org/sections/thetwo-way/2018/03/23/596341516/eu-joins-u-k-in-saying-russia-very-likely-responsible-for-nerve-agent-attack

Suicide Bombing in Kabul as Fighting Season Begins – *Terrorism*

Excerpt: An ISIS suicide bomber has struck in Kabul, killing dozens of people as they celebrated Persian new year.

The attack, which has left at least 31 dead, occurred on the road to a Shiite shrine in the Afghan capital.

The terrorist group claimed responsibility for the attack in an online statement, saying the attack was targeted at "a gathering of Shiites celebrating Nauruz".

Nauruz, as it is known in Afghanistan, is the Persian new year and a national holiday in which the minority Shiites typically celebrate by visiting shrines.

Analyst Comment: Kabul had been on alert for attacks during Nowruz, the Persian New Year. The attack took place at the Sakhi shrine, one of the largest shrines in Kabul. The shrine had previously been targeted by attacks in 2016 and 2011.

For several years, Afghanistan, Pakistan, Iraq, Syria, and other countries in the Middle East have experienced a surge in terrorist activities each spring. The winter inclement weather imposes a lull, sporadic suicide bombings, though assassinations and attacks on security forces continue. Many mountain passes between Afghanistan and Pakistan, especially in the east, become impassable as a result of snow fall. Despite the southern Afghan-Pakistani border areas typically not being affected by the snow fall, fighting slows down in Kandahar and Helmand also.

In general, a surge in terrorist activities, known as fighting season in Afghanistan, begins around the Afghani New Year in the spring. In 2016, the start of April saw the official Taliban announcement of the beginning of fighting season. Last year, the Taliban announced the start of their spring offensive towards the end of April. This suicide bombing occurred amidst the beginnings of the 2018 spring fighting season in Afghanistan.

Source: https://www.independent.co.uk/news/world/asia/kabul-bombing-latest-suicide-dead-killed-afghanistan-islamic-new-year-latest-a8266086.html

Nine Iranians Charged in Massive Cyber Theft – *Foreign Intelligence Entities*

Excerpt: Nine Iranians have been charged as part of massive state-sponsored cyber theft campaign that targeted hundreds of universities, companies and government entities in the U.S. and abroad, federal authorities announced.

The suspects, all affiliates of an Iranian-based company known as the Mabna Institute, allegedly breached the computer systems of the U.S. Department of Labor, the Federal Energy Regulatory Commission, the United Nations and the states of Hawaii and Indiana, federal officials said.

Deputy Attorney General Rod Rosenstein said Friday that the suspects allegedly stole more than 31 terabytes of data--about 15 billion pages--from 140 American universities, 30 U.S. companies and five government agencies, while targeting 176 universities abroad.

Analyst Comment: The revelations regarding Iran's expansive cyber-espionage campaign suggest a closely-coordinated operation involving a state sponsor and quasi-state actors. The campaign entails widespread intellectual property theft via cyber intrusions, focusing on information that may be of use to Iranian intelligence officials. An estimated $3.4 billion in intellectual property was stolen, including academic research in science and technological fields.

Iran's recent cyber-espionage activities are similar to the intellectual property theft perpetrated by Chinese actors (including state-sponsored activity). Intellectual property theft can include trade secrets and other sensitive information that allow those who stole the information to gain a

competitive economic advantage over the victim. Additionally, theft from entities such as defense contractors could pose a national security risk. China has been accused of stealing design information for a number of U.S. military weapons systems from the networks of defense contractors.

Similarly, in July 2017, two Iranian nationals were charged with hacking into a U.S. software firm that developed software for aerospace and defense purposes; software that is regulated under U.S. export controls for defense and dual-use technologies. Iran, China, and other nation-state or state-sponsored actors are likely to continue using cyber intrusions to gain access to intellectual property, for economic reasons as well as traditional intelligence collection purposes.

Source: https://www.usatoday.com/story/news/politics/2018/03/23/nine-iranians-charged-massive-cyber-theft-campaign-targeting-universities-justice-says/452327002/

Marine Forces Reserve Data Breach Affects Thousands – *Cyber*

Excerpt: The personal information of thousands of Marines, sailors and civilians, including bank account numbers, was compromised in a major data spillage emanating from U.S. Marine Corps Forces Reserve.

Roughly 21,426 people were impacted when an unencrypted email with an attachment containing personal confidential information was sent to the wrong email distribution list.

The compromised attachment included highly sensitive data such as truncated social security numbers, bank electronic funds transfer and bank routing numbers, truncated credit card information, mailing address, residential address and emergency contact information, Maj. Andrew Aranda, spokesman for Marine Forces Reserve said in a command release.

Analyst Comment: The recent Marine Corps Forces Reserve data breach highlights the insider threat posed by individuals who do not necessarily have any malicious intent. Rather, the breach was likely caused by human error, exposing the personally identifiable information (PII) of over 20,000 individuals. Unintentional or non-malicious insider threats may stem from inadequate training, improper oversight, or individual cases of negligence. While these insiders may lack malicious intent, they can still cause severe consequences. For example, the information compromised in the aforementioned breach could potentially be exploited by criminals (such as identity thieves), foreign intelligence entities (for targeting purposes), or terrorist groups such as the Islamic State (which has released "kill lists" containing the PII of U.S. servicemembers).

Source: https://www.marinecorpstimes.com/news/your-marine-corps/2018/02/28/major-data-breach-at-marine-forces-reserve-impacts-thousands/

Hazards

U.S. Missile Defense Base Threatened by Climate Change – *Meteorological Hazard*

Excerpt: A multibillion-dollar military installation in the Pacific that has provided key testing for the U.S. defense against a possible North Korean nuclear strike could become uninhabitable in less than two decades due to climate change.

The site, which is threatened by rising sea levels, is also used to track space junk that can cripple spacecraft.

The Army's Ronald Reagan Ballistic Missile Defense Test Site on the low-lying Kwajalein Atoll in the Marshall Islands is expected to be submerged by seawater at least once a year, according to a new study ordered by the Department of Defense. That marks a "tipping point" that could wipe out the island's source of fresh water by 2035, says the report, which was quietly released late last week.

Analyst Comment: A recent study commissioned by Department of Defense examined the anticipated effects of climate change on DoD installations around the world. Of the DoD sites surveyed, roughly 50% reported damage from 6 primary types of climate change-related natural hazards. Those hazards were: flooding due to storm surge; flooding due to non-storm surge events; extreme temperatures (both hot and cold); wind; drought; and wildfire. The risk from these and other types of natural hazards is expected to increase in coming years due to climate change, potentially threatening DoD assets' ability to accomplish their respective missions.

The Kwajalein Atoll site is a major testing site for U.S. missile defense and space research programs. The missile range, officially known as the Ronald Reagan Ballistic Missile Defense Test Site, is home to a variety of command and control facilities, missile launch facilities, tracking radars, and other equipment suitable for the installation's mission. However, rising sea levels may threaten the island on an annual basis as soon as 2035. This scenario would render a key piece of the U.S. missile defense program unusable, highlighting the potential national security risks posed by climate change.

Source: https://www.scientificamerican.com/article/key-missile-defense-installation-will-be-uninhabitable-in-less-than-20-years/

Fourth Nor'easter in Three weeks hits East Coast – *Meteorological Hazard*

Excerpt: Nor'easters along the East Coast get their name because the winds over the coastal area are typically from the northeast.

These storms may occur at any time of year but are most frequent and most violent between September and April.

Nor'easters nearly always bring precipitation in the form of heavy rain or snow, as well as gale-force winds, rough seas, and, occasionally, coastal flooding.

Nor'easters usually develop in the latitudes between Georgia and New Jersey, within 100 miles east or west of the East Coast.

The heavily populated region between Washington, D.C., Philadelphia, New York and Boston, i.e. the "I-95 Corridor," is especially impacted by Nor'easters.

These storms progress generally northeastward and typically attain maximum intensity near New England and the Maritime Provinces of Canada.

The East Coast provides an ideal breeding ground for nor'easters. During winter, the polar jet stream transports cold, Arctic air southward across the plains of Canada and the United States, then eastward toward the Atlantic Ocean where warm air from the Gulf of Mexico and the Atlantic tries to move northward.

The warm waters of the Gulf Stream help keep the coastal waters relatively mild during the winter, which in turn helps warm the cold winter air over the water. This difference in temperature between the warm air over the water and cold Arctic air over the land is the fuel that feeds nor'easters.

Analyst Comment: Four powerful Nor'easter storms have hit the United States' Eastern Coast this March. While it is somewhat rare to see so many nor'easter storms in a row, they are not uncommon for this time of year and part of the country. A little more than three years ago, there was a similar occurrence of three strong coastal storms passing near this benchmark over the span of a week and a half. Nor'easters are a common type of storm during the winter and early spring months along the Atlantic coast of the U.S.

Reoccurring heavy snows and wind have caused millions of power outages, coastal flooding, lake shore flooding, and damaging winds. Major airline, train, and public transit delays occurred throughout the month, all along the east coast. The continuous buildup of snow is also potentially dangerous to any weakened structures or trees.

Winter Storm Riley began March 2nd with destructive winds, heavy snow and severe coastal flooding in the Northeast. Winter storm Quinn followed shortly thereafter, bringing more heavy snow. Winter Storm Skylar hammered the Northeast corridor on March 13th, with heavy snow, damaging winds and minor coastal flooding. Winter Storm Toby was the fourth nor'easter to hit in less than three weeks, bringing heavy snow and some winds. Toby dumped a foot or more of snow in at least five states, with heavy snow stretching from Long Island to the Appalachians to parts of the Ohio Valley.

Source: http://abcnews.go.com/US/east-coast-braces-noreaster-storm/story?id=53437715

CDC Warns of Second Wave of Flu – *Biological Hazard*

Excerpt: Although the flu season is coming to an end, officials with the Centers for Disease Control and Prevention said that in recent weeks, a second wave of the deadly influenza virus has emerged.

In its weekly flu report, issued on 23 March, CDC officials said they saw a decline in overall influenza cases for the week ending 17 March. The decline was particularly apparent for the A-strain of the virus, which has been dominant since the flu season started in October.

However, officials noted that they've seen more reports of the flu virus's B-strain, which has been slowly overtaking reports of influenza A. For the week ending 17 March, influenza B made up about 58 percent of the week's total flu reports.

Analyst Comment: Per the CDC, flu viruses are most common during the fall and winter. The exact timing and duration of flu seasons can vary, but influenza activity often begins to increase in October. Most of the time flu activity peaks between December and February, although activity can last as late as May.

This "second wave" of influenza B observed by CDC is still within the parameters of typical influenza season, although public health concerns remain. Individuals can become sick by both influenza A and influenza B strains within the same season, and influenza B is especially dangerous to children. A CDC spokesperson advised that individuals should still consider getting a flu shot despite it being later in the season, as the vaccine is recommended as long as the virus is still circulating.

Source: https://www.ajc.com/news/national/cdc-warns-second-wave-flu-virus/28y7M3DEPu7n4fDvd18YaI/

In the Spotlight

'In the Spotlight' is designed to highlight a threat or hazard event, or associated events, that have been observed over recent history, and provide contextual analysis and trend based analysis on these events.

The Austin Bomber

Throughout March, a series of bombings was carried out in Austin, Texas. Each of the packaged bombs varied in trigger and delivery method. The Austin Police Department warned citizens to take precautions against unexpected packages. The department reported having responded to more than 1,250 calls about suspicious packages between March 12th and March 20th.

On March 2nd, a package left on the front porch of his house killed Anthony Stephan House. On March 12th another package was left on the front porch and brought inside of the Mason family home, where it killed Draylen Mason and injured one other. Another woman is severely injured after picking up a package left near her home. After the second bombing, law enforcement had to evaluate if the bombings were all connected to the SXSW festival going on in the city at the time. And because the first victims had been African American and Latino, law enforcement also considered whether the bombings were racially motivated. Law enforcement agents eventually concluded the bombings were unrelated to the SXSW festival. And after another bomb went off and added white victims, Austin law enforcement expanded their investigation.

On March 18th two men are injured in an explosion while walking on a sidewalk. The explosion was triggered by a tripwire connected to a bomb that was anchored to a for-sale sign. On March 20th a package exploded while inside a FedEx sorting facility, resulting in one injury. Later that morning, a package containing an explosive device was identified and secured at another FedEx facility. That evening an explosion occurred at a Goodwill. However, this incident was determined to be unrelated to the other bombings.

Later that day, a suspect, Mark Anthony Conditt, was identified. That afternoon of the 20th paramedics were notified about an "unknown medical alarm" at Mr. Conditt's home in Pflugerville. Two paramedics from the Pflugerville Fire Department responded. A person inside the home — it was unclear whom — answered the door and told the medics no one there had called 911. From an incident report released Friday by the Pflugerville Fire Department, it now appears that a request by investigators for paramedics to remain near the house was relayed instead as a call for immediate medical aid to the residence. It is possible that Mr. Conditt himself had come to the door or was home at the time, and began to suspect that the authorities were closing in.

On March 21st the suspect, Mark Anthony Conditt, was tracked to a hotel outside of Austin. As he drives away from the hotel, law enforcement followed. The car then pulled into a ditch and the suspect detonated a bomb inside the car, killing himself.

When searching Conditt's home, investigators discovered components for making similar bombs to the ones that exploded in the past few weeks. The devices that exploded in Austin and near San

Antonio were pipe bombs with batteries and smokeless powder and were constructed with materials found in a hardware or sporting goods store. The bombs had distinctive shrapnel inside. Some had "mousetrap" switches and others had "clothespin" switches.

Homemade explosive devices can be created relatively simply from common goods, such as pool sanitizers, fertilizers, and paint removers. Simple explosives are generally made by combining an oxidizer with a fuel, while more complicated explosive devices may use a variety of triggering methods as well as additional materials to inflict further damage, such as the distinctive shrapnel contained in Conditt's devices. There are several websites that purportedly contain instructions or 'recipes' on how to make a homemade bomb. Conditt's ability to create and distribute homemade explosive devices reflects the relative ease with which domestic actors can acquire the needed materials and distribute the devices.

Over the past ten years, many homemade explosive devices have been successfully created within the U.S. Some have been detected and disarmed, some were discovered before distribution, and some were successfully distributed and detonated. In the future, other domestic actors will continue to have the ability to create and distribute homemade explosive devices and inflict damage to chosen targets.

Conditt's use of package delivery to distribute bombs is a tactic that can easily inflict damage upon a majority of homes, businesses, and heavily trafficked areas. If DoD personnel are targeted, explosive packages could be sent to their homes, work, or locations known to be frequented by DoD.

Later, it was reported that the suspect left a video confession, describing seven explosive devices but revealing no clear motive. The FBI defines domestic terrorism as "perpetrated by individuals and/or groups inspired by or associated with primarily U.S.-based movements that espouse extremist ideologies of a political, religious, social, racial or environmental nature." Conditt used premeditated acts to inflict terror upon civilians. However, due to the current lack of a motive, it is difficult to clearly classify him as a domestic terrorist at this time. The packaged bombs exploding in Austin didn't show an immediately clear pattern of attack — victims were racially diverse, package delivery method evolved, and bomb triggers varied.

Sources:

https://www.cnn.com/2018/03/25/us/austin-bombings-investigation/index.html

http://www.kvue.com/article/news/local/verify/verify-why-isnt-the-austin-bomber-being-called-a-terrorist/269-531179612

https://www.nytimes.com/2018/03/23/us/austin-bombing-targets.html