Risk Mitigation Consulting Inc.

Intelligence and Analysis Division

OPEN SOURCE UPDATE

6 August 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

Islamic State Returns to Assassination Tactics – *Terrorism*

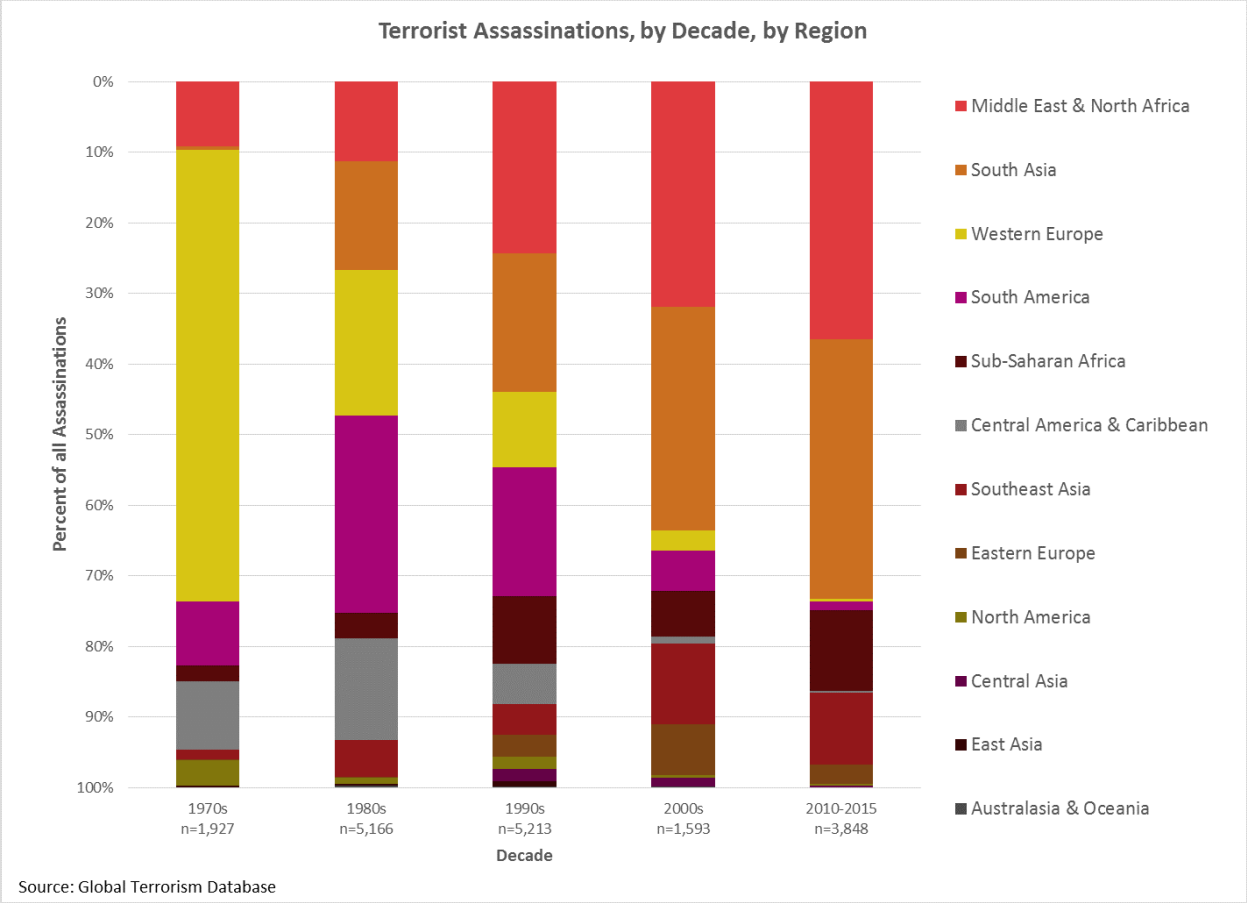
Excerpt: Roughly four years ago, ISIS shocked the world when it took over a large swath of territory across Iraq and Syria, declaring the establishment of a new Islamic caliphate in the process.

Fast forward to 2018 and the terrorist group is a shadow of what it was even a year ago. It has lost the vast majority of the territory it previously held and the number of fighters it counted among its ranks has dwindled exponentially to below 3,000.

Nevertheless, ISIS remains a threat in the Middle East, and a new report from the Soufan Center warns it's attempting to make a comeback by resorting to a tactic it employed back in 2013 when it was still known as Al Qaeda in Iraq (AQI) — the targeted assassinations of Iraqi security personnel.

Analyst Comment: The Soufan Center's report on ISIS (also known as the Islamic State, or IS) states that the terror group has recently increased its targeting and assassinations of police personnel in Iraq, including an attack in June that killed 8 members of Iraqi security forces. This tactic is likely a result of the group's struggle to maintain power in the wake of a drastic loss of territory over the past few years. Assassinations do not require territorial control, require a low number of personnel to conduct, and are relatively simplistic and low-cost when compared to other terrorist tactics. IS' latest assassination campaign is similar to past assassination campaigns by the group, which are designed to intimidate security forces and undermine the public's confidence in the government's ability to protect them.

A 2017 analysis conducted by the National Consortium for the Study of Terrorism and Responses to Terrorism (START) found that a majority of worldwide assassinations by terrorists took place in the Middle East/North Africa and South Asia in recent years. The percentage of worldwide terrorist assassinations by region since the 1970s has also gradually shifted decade-over-decade from a majority of assassinations in Western Europe to the majority in the aforementioned two regions. (See Figure Below)



Source: https://www.businessinsider.com/isis-trying-to-make-a-comeback-by-creating-chaos-with-assassinations-2018-7

Venezuelan President Maduro Drone Assassination Attempt – *Terrorism*

Excerpt: Authorities have identified the masterminds of the apparent drone assassination attempt on Venezuelan President Nicolas Maduro, as well as the people who assisted them, Attorney General Tarek William Saab said Monday.

The investigation, which involves four prosecutors, has yielded the locations from where the drones were piloted, as well as the arrests of two of the drone pilots, the country's top law enforcement official said.

"We also know the places where they stayed in the days leading to the attack. We have identified the people who made the explosives and prepared the weapons and their international links," Saab said.

Analyst Comment: According to local investigators, the individuals behind the attack are known to the Venezuelan Government; one had an active arrest warrant for a 2017 attack on a military installation in the country, while another was arrested for anti-government protesting in 2014. During the attack on the Venezuelan President, explosive laden drones flew overhead with the intent to detonate within range of the president. However, the attack was foiled when one drone didn't explode in range and the other flew into a building.

The drones used were Chinese made DJI M600 drones, each loaded with 1kg of C4 explosive. According to the manufacturer, this model drone has a maximum payload of 6kg and comes equipped with a GPS-compass, a maximum transmission range of 5km, with a maximum flight time of 40 minutes. However, if fully loaded this flight time is reduced to 15 minutes. In the case of the attack against the president, the drones would have had a maximum flight time of 30 – 35 minutes. Per their website, the drone is designed for "professional aerial photography and industrial applications."

This is prime example of a terrorist group using explosive laden drone tactics to carry out an assassination attempt. While instances of assassination attempts in South America have declined significantly since the 80's, they are still an option for terror groups operating in the region; particularly as emerging technology continues to become available to the average consumer. Similarly, assassination attempts have been decreasing in North America since the 70's. However, increased drone availability and usage, along with the copy-cat mentality, could potentially cause an increase in illicit drone targeting by lone actors or HVEs in the Homeland.

Source: https://www.cnn.com/2018/08/06/americas/venezuela-maduro-apparent-assassination-attempt/index.html

Chinese Spy Ship Monitoring RIMPAC Exercise – *Foreign Nation-State Military*

Excerpt: A Chinese surveillance ship is operating off the coast of Hawaii to keep tabs on the U.S.-led Rim of the Pacific (RIMPAC) exercise, a Navy official confirmed to USNI News on Friday.

The People's Liberation Army Navy's (PLAN) auxiliary general intelligence (AGI) ship has been operating in the exclusive economic zone (EEZ) off the coast of Hawaii since July 11, U.S. Pacific Fleet spokesman Capt. Charlie Brown told USNI News on Friday.

"We expect the ship will remain outside the territorial seas of the U.S. and not operate in a manner that disrupts ongoing RIMPAC exercise," Brown said.

"We've taken all precautions necessary to protect our critical information. The ship's presence has not affected the conduct of the exercise."

Analyst Comment: RIMPAC is a multilateral military exercise that takes place every two years, and is hosted by the U.S. Several additional nations are invited to the exercise, including a number

of U.S. allies (such as South Korea and Japan) and more recently, China. China was first invited to RIMPAC in 2014 and participated in 2016 despite ongoing tensions with the U.S. regarding the South China Sea. In 2018, the U.S. revoked China's invitation to RIMPAC, with the Pentagon citing China's military buildup in the South China Sea as the reason behind the revocation.

Although the Chinese ship currently remains outside of U.S. territorial waters, it reportedly remains in close proximity to the RIMPAC exercise. The presence of the Chinese vessel (which, according to a Navy spokesman, is a surveillance ship), is likely a provocative military response to the U.S. disinvitation as well as a potential intelligence collection platform. While the Navy spokesman stated that "all precautions necessary" have been taken to protect critical information and that the ship has not "affected the conduct of the exercise," the exact capabilities of the Chinese vessel are unknown, and the threat of intelligence collection should not be discounted entirely. Still, the vessel's presence may escalate military tensions by provoking a future U.S. response (such as the deployment of U.S. vessels to the South China Sea).

Moreover, the presence of foreign naval vessels in vicinity of U.S. military exercises is not uncommon, as they typically remain within the bounds of "freedom of navigation" under international law. China sent a similar vessel to the 2014 RIMPAC exercise, while a Russian spy ship was spotted near RIMPAC in 2016. Similarly, a Russian surveillance vessel called the Viktor Leonov has been spotted making regular deployments up and down the U.S. East Coast in recent years, transiting in close proximity to U.S. military installations.

Source: https://news.usni.org/2018/07/13/navy-chinese-spy-ship-monitoring-rimpac-exercise

Hacker Caught Selling Maintenance Manuals for Military Drones – *Cyber*

Excerpt: Until last week, you could have purchased one of the U.S. military's training manuals for the MQ-9 Reaper drone, along with a maintenance manual for the Abrams tank, a guide to defeating IEDs, and other sensitive materials, thanks to a hacker who put the stolen materials up for sale online.

The theft and attempted sale were brought to light by cybersecurity and threat intelligence group Recorded Future, which published a report about the incident and is working with law enforcement personnel on it.

Recorded Future officials said they got involved last week when they noticed a suspicious-looking online advertisement for the manuals, a list of airmen within a unit assigned to the drone's maintenance, and more. They contacted the thief, who said that he had hacked his way to the materials after an Air Force captain with the 432d Aircraft Maintenance Squadron at Creech Air Force Base in Nevada failed to properly set transfer protocol settings on his NETGEAR router, a widely-known vulnerability. The hacker used a search engine called Shodan that allows users to search unsecured Internet of Things devices and happened upon the captain's router by chance,

whereupon they used the vulnerability to exfiltrate the docs from the captain's computer, including—awkwardly—his certificate of completion for Cyber Awareness Challenge Training.

Analyst Comment: Recorded Future's report states that its analysts first discovered the documents posted for sale on a hacking forum, and subsequently established contact with the individual who stole the documents. The hacker had reportedly gained access to a DoD servicemember's computer by exploiting a widely-known hardware vulnerability for a particular internet router for some documents and an unknown hacking technique to steal the others. The incident highlights the importance of maintaining a robust cybersecurity program for hardware and software, as well as regular awareness training for personnel. While none of the documents contained classified information, they contained information that would likely be appealing to malicious actors, such as maintenance information for weapons systems such as the MQ-9 Reaper drone and the M1 Abrams tank. The hacker posted these and other documents for sale on an open forum, where they could potentially by acquired by terrorist, criminal groups, or foreign intelligence entities.

Based on the available information, this incident does not appear to have initially targeted the U.S. military specifically. Rather, the hacker reportedly used a search tool that identified unsecured devices in the "internet of things," or IoT, and found the servicemember by mere chance. It is unclear how much sensitive U.S. government information is obtainable through similar techniques, but it is likely a fairly repeatable process. Recorded Future is currently cooperating with law enforcement and the Defense Security Service (DSS) regarding the incident, and Recorded Future indicated in its own report that military response teams will "determine the exact ramifications".of the breaches.

Source: https://www.defenseone.com/technology/2018/07/hacker-caught-selling-maintenance-manuals-military-drones/149614/

Hazards

2018 on Pace to be the 4th-Hottest Year on Record – *Meteorological Hazard*

Excerpt: According to data from the National Oceanic and Atmospheric Administration (NOAA), 2018 is on pace to be the fourth hottest year on record. Only three other years have been hotter: 2015, 2016 and 2017.

The upward trend is not lost on experts, who say the rising temperature is a clear indicator of global warming.

"The impacts of climate change are no longer subtle," said Michael Mann, a climate scientist and director of the Earth System Science Center at Penn State University.

"We are seeing them play out in real time in the form of unprecedented heat waves, floods, droughts and wildfires. And we've seen them all this summer," he said.

Analyst Comment: A hotter-than-usual year in 2018 has been marked by a variety of global weather phenomena that some have dubbed a "global heat wave." Several climate scientists have linked the global increase in temperatures to a variety of severe meteorological conditions around the globe including record temperatures, drought and wildfires, and flooding induced by heavy rains. Examples of such conditions include record temperatures recorded in the Arctic Circle, historic flooding in Japan, and drought conditions in the United Kingdom. In the U.S., wildfires raged throughout the Western portion of the country (particularly in California), while heat waves caused electrical grid concerns in major metropolitan areas. However, the effects of climate change can also exacerbate the effects of normal meteorological hazards in the colder months. Extreme cold temperatures and heavy snow can also be attributed to the effects of climate change to some degree. However, it is worth noting that individual, local events do not serve as indicators of climate change. Rather, trend analysis of global patterns must be conducted over a long period of time in order to draw such conclusions.

Source: https://www.cnn.com/2018/07/28/us/2018-global-heat-record-4th-wxc/index.html

California Wildfire Generates Its Own Weather System – *Meteorological Hazard*

Excerpt: The tower of billowing cumulus clouds and smoke rising above Northern California's Carr fire said it all. The flames jumping around Redding's western edge had created their own micro weather system, tossing fire brands helter-skelter across the baking landscape.

California's big, destructive wildfires tend to come in two varieties: wind-driven, such as last year's deadly Santa Rosa conflagration and December's Thomas fire in Southern California. And

what is known as plume-dominated, when a fire's plume of smoke and ash is big and hot enough to exert control.

Wind gusts were a factor in the Carr, which destroyed 65 residences on Redding's edge, sent panicked homeowners fleeing in the middle of the night and caused the deaths of a city firefighter and a bulldozer operator. But fire experts say the explosive growth of the Carr was more a function of extreme heat and dried-out fuels that stoked flames intense enough to generate their own weather.

Analyst Comment: As of 31 July 2018, the Carr fire is the seventh-most destructive fire in California history, with more than 170 square miles burned and roughly 900 homes destroyed in the blaze. However, the fire is also producing unique, hyper-local meteorological conditions, which some analysts have described as "the fire creating its own weather system." This phenomenon is created by "pyrocumulus clouds," which occur during wildfires as well as volcanic eruptions. According to Outside magazine, these clouds form when "the intense heat of a huge wildfire burns the moisture out of the vegetation". The moisture then "accumulates on smoke particles and rapidly condenses as it rises." The temperature variations caused by the formation of these clouds can then lead to unpredictable, severe winds that can rapidly affect fire conditions on the ground, endangering first responders and the public alike.

However, the Carr fire is only one of a number of wildfires currently raging throughout California. As of 31 July 2018, 16 active fires are burning in the state, and several additional fires are occurring throughout the Western U.S. Per the National Fire Incident Reporting System (NFIRS)'s Significant Wildland Fire Potential Outlook for August 2018, much of California, Nevada, Utah, Idaho, and Montana and the entirety of Oregon and Washington are designated as having "Above Normal" fire potential. NFIRS also notes that August represents the peak of the Western Fire Season.

Source: http://www.latimes.com/local/lanow/la-me-california-wildfire-year-20180728-story.html

Swine Fever Epidemic in China – *Biological Hazard*

Excerpt: China's Liaoning province will increase inspections at pig farms and markets and strengthen the monitoring of hog transportation, after the nation's first African swine fever case was reported there, local media Liaoning Daily reported on Monday.

The African swine fever outbreak poses a major threat to the hog farming industry in the province and the whole country, and must be eradicated thoroughly, an official from Liaoning Provincial Bureau of Animal Health and Production said, according to Liaoning Daily.

The provincial government has asked local authorities to launch emergency inspections at all pig farms, hog markets, slaughterhouses and harmless treatment sites in the province, and report any cases of pig deaths due to unknown reasons, slaughtered pigs found with splenomegaly or splenic hemorrhage, and immune failure among pigs after receiving swine fever vaccines, the paper reported, citing the animal health bureau.

Analyst Comment: African swine fever (ASF) is a highly contagious viral disease; however, it is limited to members of the pig family which includes domesticated and wild boars. The virus is generally only found in Africa, but outbreaks have occurred in Europe, and Latin America. ASF has never occurred in the U.S., and this is the first such case in China and greater East Asia. Signs of ASF vary but often include high fever, decreased appetite and weakness. The skin may be reddened, blotchy, or have blackened lesions, and infected pigs may also have diarrhea, vomiting, etc. Pigs primarily get the disease through infected ticks, flies, or other insects. Death can be anywhere from sudden to 10 days after exposure, while pigs that recover can carry the virus for several months.

However, as previously stated, humans are not susceptible to ASF directly. The most likely threat from this viral outbreak in East Asia is to other pigs and the pork industry. Mainland China produces 50% of the worlds pork, but because of internal demand it only accounts for roughly 0.9% of the worlds swine exports (making it 18th ranked, while the U.S. is ranked 2nd at 15.2% of the worlds exports.) The major concern is the outbreak spreading further in China, or to other East Asian countries with North Korea located roughly 80 miles from the outbreak zone. Additionally, this has caused Japan to suspend imports of heat-treated Chinese pork and tighten quarantine operations at airport and seaports. Should this disease, which was previously unknown to the region, continue to spread to Chinese pork export nations there could be additional ramifications on the regional swine population.

Source: https://www.reuters.com/article/us-china-swineflu-pigs-measures/china-to-launch-emergency-inspections-on-farms-after-swine-fever-outbreak-idUSKBN1KR136?feedType=RSS&feedName=healthNews