Risk Mitigation Consulting Inc.

Intelligence and Analysis Division

OPEN SOURCE UPDATE

March 2020

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

CIA Software Engineer on Trial for Sharing Agency Secrets With WikiLeaks – *Insider Threat*

Excerpt: Federal prosecutors said that a software engineer on trial for the largest leak of classified information in CIA history was "prepared to do anything" to betray the agency.

Joshua Schulte is a former CIA coder accused of sending the anti-secrecy group WikiLeaks a large portion of the agency's computer hacking arsenal — tools the agency had used to conduct espionage operations overseas.

"The defendant was prepared to burn down the United States government," Assistant U.S. Attorney Matthew Laroche said. "He is an angry and vindictive man."

His defense attorney argued the man had been scapegoated for a breach that exposed secret cyberweapons and spying techniques.

Prosecutors have said the leak was devastating to national security, as it exposed CIA operatives, brought intelligence gathering to a halt and left allies wondering whether the U.S. could be trusted with sensitive information.

Schulte left a trail of evidence despite learned attempts to erase his digital fingerprints, Laroche said in closing arguments. Schulte became disgruntled at the CIA, he said, and took meticulous steps to plan — and cover up — the 2016 theft.

"He was the only one who had the motive, the means and the opportunity to steal the information," Laroche said. "He was prepared to do anything to get back at the CIA."

Analyst Comment: Although the merits of the case were vigorously debated and Schulte was ultimately convicted on lesser charges (making false statements and contempt of court), this incident involves many indicators that suggest insider threat activity. Schulte reportedly engaged in a variety of suspicious activities, to include deleting computer logs and restoring administrator privileges to systems which he did not have authorized access to. Additionally, according to prosecutors, Schulte reportedly searched for the information he is accused of leaking on WikiLeaks on "dozens" of occasions. In recent years, WikiLeaks has hosted classified information leaked to it in high-profile cases by individuals to include Chelsea Manning and Edward Snowden, among others.

Source: https://www.foxnews.com/us/prosecutors-describe-ex-cia-engineer-charged-in-massive-leak-as-angry-and-vindictive

State Dept. Wants to Designate Atomwaffen Division as Terrorist Group – *Terrorism*

Excerpt: The State Department is pushing to designate at least one violent white supremacist group as a foreign terrorist organization, an unprecedented move that national security experts say would be a big step toward fighting a growing threat on U.S. soil.

State Department officials want to have the designation finalized by next week, according to four people familiar with the effort. But the White House, where top officials have long preferred to focus on terrorism by Islamist extremists, has yet to give the green light.

Former U.S. officials and counterterrorism analysts say the top candidate for the designation is Atomwaffen, a neo-Nazi group that was founded in the United States but has expanded into the United Kingdom, Canada, Germany and Estonia.

Designating Atomwaffen or another neo-Nazi group like The Base as a terrorist outfit would send a major signal that the U.S. views far-right terrorism as a rising danger that increasingly ignores national boundaries, thanks in no small part to the internet.

The FBI arrested five alleged Atomwaffen members last month and eight alleged members of white supremacist group "the Base" in January. Six members of Atomwaffen have been convicted since 2018 on charges including planning terrorist attacks and murder.

Analyst Comment: Atomwaffen Division (AD) began on the now-defunct *IronMarch.com* in 2015. Its former members have been associated with far-right violence in the United States and Europe. AD's leader, John Denton, was recently arrested in Virginia on a "swatting" charge against a *ProPublica* journalist who had revealed his identity. Swatting is the practice of calling the police and reporting a violent crime in progress at a victim's address, with the intention of summoning a SWAT team. Denton has a history of swatting for both mischief and intimidation.

AD is somewhat unique among alt-right groups in that it advocates the destruction and downfall of the United States. Members have burned the Constitution in videos online and praised countercultural and criminal individuals, including neo-Nazi writer James Mason and murderer Charles Manson. The group attracts recruits from the ranks of active duty military, universities, and even high schoolers. Several members have been involved in acts of violence, including murder. Unlike other so-called "keyboard warriors" that populate alt-right and hate sites, AD encourages acts of violence against both civilian and government targets. A recent leak of user information from *IronMarch.com* may make it easier for federal authorities to arrest its members. Designating the group as a terrorist organization will make it even more so.

Source: https://www.politico.com/news/2020/03/09/state-department-white-supremacist-group-124500

3 Dead in 'Active Shooter' Situation in Huntersville, NC – *Active Shooter/Active Assailant*

Excerpt: Police say three people are dead after they were called to a house in a Huntersville neighborhood for a "active shooter" situation early 13 March 2020 just before 6 a.m. in the Vermillion neighborhood on ES Draper Drive. Police said they were called to the house for reports of an assault with a deadly weapon. When they first got to the house, they were not able to enter but the SWAT team was standing by.

Officers encouraged residents to stay inside their homes and shelter in place. Huntersville police have not identified the three victims or said if there was any relationship between them. Authorities have not said what led up to the shooting, but did say that they are not looking for any suspects.

Officers said they started evacuating nearby homes around 6 a.m. out of caution. Residents said the neighborhood is very tight-knit and everyone knows everyone so the news is devastating.

Analyst Comment: Usually the phrase "active shooter" invokes the image of an assailant in a public space (such as a school campus or at a mall) indiscriminately firing at anyone in their path. This incident in Huntersville shows that the definition has broadened over time. The FBI defines an active shooter as "an individual actively engaged in killing or attempting to kill people in a populated area[.]" While the shooter in Huntersville was inside a house, police efforts to tell residents to, first, shelter in place and, then, to evacuate shows how a domestic shooting can escalate. While we know little about the shooter or the victims, police were clearly afraid the shooter would leave the residence and open fire in the streets. This could potentially demonstrate a change in tactics and perspective following the rash of mass shootings in the United States over the past decade.

This follows a string of active shooter alerts and threats at a series of malls over the past four days. On 10 March, in College Station, TX, local law enforcement responded with active shooter protocols to a simple robbery at a mall jewelry store. Three men attempted a "smash and grab." Some witnesses mistook the sound of glass breaking in the store for gunfire and called the police. After locking down the mall and investigating, police determined there was no active shooter. The suspects are still at large, though their vehicle was later found abandoned.

On 11 March, an individual threatened to open fire at a San Jose mall on the Internet forum Reddit. The individual has, apparently, a history of making non-credible threats and is under investigation. On 12 March, police arrested a different individual at a different mall in San Jose, following social media reports of an active shooter. No details were available, but no shots were fired.

The swift implementation of active shooter protocols demonstrates that local law enforcement has adapted to the unfortunate "new normal" of active shooters and mass shootings in public spaces. While this is tragic, local agencies should continue to train and prepare for the potential for an active shooter event occurring in their jurisdiction, as such events are often difficult to predict.

Source: https://www.wsoctv.com/news/local/residents-told-leave-homes-medic-police-respond-shooting-huntersville-neighborhood/R3KPHNOJV5BL5BS3SMBMKQOBKU/

U.S., Canadian Fighter Jets Intercept Russian Spy Planes Near Alaska – *Foreign Nation-State Military*

Excerpt: Two Russian Tu-142 maritime reconnaissance aircraft lingered in U.S.-Canadian air defense space Monday [09 March] for hours after being intercepted by fighter jets, defense officials said.

The two Russian planes were intercepted by U.S. Air Force F-22 Raptors and Royal Canadian Air Force CF-18s, a version of the U.S. Navy's F/A-18 Hornet, in the Alaskan Air Defense Identification Zone, officials said in a release.

The ADIZ surrounds the United States and Canada, stretching west of Alaska to cover the Semichi Islands, south of Russia. It's jointly defended by both countries, and foreign aircraft are not permitted to fly alone in ADIZ airspace without authorization.

The F-22s and CF-18s were supported by U.S. KC-135 Stratotanker refueler and E-3 Sentry airborne early warning and control aircraft, officials said.

"[North American Aerospace Defense Command] fighter aircraft escorted the Tu-142s for the duration of their time in the ADIZ," officials said. "The Russian aircraft remained in international airspace over the Beaufort Sea, and came as close as 50 nautical miles to the Alaskan coast. The Russian aircraft did not enter United States or Canadian sovereign airspace."

Officials did not say that the Russian planes acted unprofessionally in the space or otherwise presented a threat.

Analyst Comment: Russia has a demonstrated history of flying military aircraft into the U.S. ADIZ near Alaska, prompting interceptions by U.S. and Canadian aircraft. Russia typically flies heavy bomber aircraft or reconnaissance aircraft in close proximity to U.S. airspace, with likely goals to include provocation or a ”show of force,” testing of U.S./Canadian response, and potentially foreign intelligence activities (considering the choice of aircraft such as the Tu-142. Most incursions typically involve Russian planes acting “professionally” by adhering to interceptions/escorts by U.S./Canadian jets without any overt threats or irresponsible maneuvers.

Per open source reporting, the Tupolev Tu-142 is a maritime reconnaissance and anti-submarine warfare plane derived from the Tu-95 “Bear” strategic bomber. The Tu-142 can be outfitted with various radars, communications systems, and anti-submarine warfare equipment in order to perform a variety of mission sets.

Source: https://www.military.com/daily-news/2020/03/10/us-canadian-fighters-intercept-russian-spy-planes-north-alaska.html

Hackers Use Coronavirus Fears to Steal Data – *Cyber*

Excerpt: Chinese hackers have used fake documents about the coronavirus to deliver malicious software and steal sensitive user information, according to a report Thursday from researchers documenting a growing wave of cybercrime exploiting fears about the global pandemic.

As the novel coronavirus has moved across the world, cybercriminals and spies have taken advantage of the growing demand for information by loading malicious software into tracking maps, government reports and health fact sheets in numerous languages. New websites with variations on "coronavirus" in their Internet addresses also have exploded, with many of them masking online scams.

In recent weeks, U.S. officials have warned about malicious actors seeking to seize on global coronavirus concerns to peddle fraudulent products or extract sensitive information. Last week, for example, a top cybersecurity arm at the Department of Homeland Security flagged the potential that criminals and hackers "may send emails with malicious attachments or links to fraudulent websites to trick victims into revealing sensitive information or donating to fraudulent charities or causes."

Analyst Comment: The responsible group, "Vicious Panda," appears to have ties to the Chinese government and is classified as an Advanced Persistent Threat (APT), meaning it plays a "long game" with its targets. This was uncovered by the cyber intelligence firm Check Point Research. Vicious Panda targeted a public sector entity in Mongolia. The e-mails attachments were purported to be press briefings from the Mongolian Minister of Foreign Affairs. Instead, they contained remote access malware. China's choice of targets is interesting. Most Mongolian exports are either bought by China or transported through it. The two countries are allies, although the smaller country has to maintain a balance with Russia and the larger international community.

In early February, Mongolia closed the border in response to the coronavirus. It repatriated 31 citizens from Wuhan, all uninfected. Mongolia is in the process of repatriating citizens from South Korea and elsewhere. As of 12 March, the country has only had one confirmed case. China is known for its persistent espionage against even its most active trading partners. This could be an effort to disrupt or otherwise encumber Mongolia's public sector in retaliation for extracting its citizens from Wuhan. But "Vicious Panda" has been responsible for malware attacks against Russia, the Ukraine, and Belarus dating back to 2016. Their most recent effort is in line with those of hackers worldwide, in that they use the fear surrounding the coronavirus to phish or otherwise lure targets. Cybersecurity fundamentals are in order here. E-mail recipients should carefully examine attachments and links to avoid being victimized by hackers.

Source: https://www.washingtonpost.com/technology/2020/03/12/hackers-are-using-coronavirus-fears-target-people-looking-information-infection-maps/#comments-wrapper

Thousands in Italy Try to Flee Coronavirus Quarantine After Leak – *Civil Disturbance*

Excerpt: Thousands of people rushed to flee Northern Italy after plans by the government for a 16-million-person quarantine were leaked to the media ahead of time.

Italy on Sunday [08 March] shut down its Northern Lombardy region, which includes Milan, and 14 nearby provinces, a lockdown that is due to last until at least 03 April 2020.

The measure does not totally restrict movement within the areas, but it means places like schools, museums, and theaters are closed, events like weddings and funerals are suspended, and bars and restaurants must keep customers a minimum distance apart.

People can enter or leave the affected area only for emergencies, with the possibility of jail time for those who break the rules.

A draft of the bill to enforce the rules was reported by the Italian newspaper Corriere della Sera on Saturday [07 March], prompting panic and pushing thousands of people to try to leave the region before the measures took place.

Analyst Comment: The Italian government's quarantine comes following the more than 7,300 confirmed COVID-19 cases and 366 deaths, making it the highest in Europe. This follows in the steps of the Chinese government's decision to "lock down" the city of Wuhan three weeks ago, quarantining 11 million people. Like the Wuhan quarantine, the citizens of Northern Lombardy are allowed to, but are discouraged from, leaving their homes. However, residents of the Northern Lombardy region are also not allowed to travel beyond its borders, except for emergencies.

These restrictions are concordant with best practices. Minimizing contact between individuals who may not have symptoms of the virus while it "runs its course" However, the longer a quarantine lasts, the greater the potential for civil unrest grows. Italian authorities have already reported escapes, protests, and general unrest at five prisons in Modena, Pavia, Foggia, and Rome. This included outside agitators setting fire to the Rebibbia prison, which facilitated the escape of 30 inmates. All were later captured by Rome police forces. While unrest at prisons is hardly surprising, as supplies run low in quarantined areas and citizens become restless, the potential for protests, rioting, and looting increases dramatically. The citizens of Wuhan have been quarantined since 23 January at home, in hotels, and in field hospitals. Citizens have reached Western media to inform them of the harsh and increasingly desperate conditions in the city, undermining the Chinese government's traditionally guarded approach to releasing information.

Source: https://www.businessinsider.com/coronavirus-italy-lockdown-plan-leaked-thousands-tried-to-flee-2020-3

Drone Bombings Target U.S. Troops in Syria – *UAS*

Excerpt: Drones are dropping explosives on US soldiers in Syria, and it's not clear who's behind the attacks, the head of US Central Command, which is responsible for the region, told lawmakers on Tuesday [10 March].

National Public Radio reporter Tom Bowman first reported the attacks on Friday, observing them as he joined a patrol by US soldiers tasked with protecting oil fields in northeast Syria.

"It was a multiday attack on two of the oil fields, the first one since the US mission began last fall to protect the oil fields," Bowman said on All Things Considered. "There were soldiers from the West Virginia National Guard at one of the fields. And early Wednesday morning, a drone carrying a mortar dropped it near where they were sleeping. No one was injured, and the soldiers quickly drove off the base."

Bowman said Army investigators had told him that some of the mortars "were made with 3D printers, which means that obviously someone pretty sophisticated put together these mortars, perhaps a nation-state."

Analyst Comment: Drones present a growing threat to U.S. forces abroad. There is a history of the Islamic State terrorist group using drones in attacks. Furthermore, they have produced propaganda of these UAS dropping bombs in Iraq and Syria. Several other groups in Syria and Iraq, including the Iraqi government, have been reported to use these small drone attacks.

Enemy UAS have expanded in size, sophistication, range, lethality and numbers since their initial use in 2014. A growing number of consumers use commercially available hobbyist drones, as they are small, cheap, and easily accessible. This growing accessibility parallels an increased use of small drones in attacks by terrorist groups. Additionally, the use of 3-D printed mortars and drone components may lead to more rapid expansion of this weapon use. To date there have been no drone attacks on military installation or personnel within the U.S.

Source: https://www.businessinsider.com/drones-used-to-drop-bombs-on-us-troops-in-syria-2020-3

Hazards

Chronic Flooding, Earthquakes in Jakarta – *Geological/Meteorological Hazards*

Excerpt: Floods that have crippled much of Indonesia's capital worsened Tuesday [25 February], inundating thousands of homes and buildings, including the presidential palace, and paralyzing transport networks, officials and witnesses said.

Overnight rains caused more rivers to burst their banks in greater Jakarta starting Sunday [23 February], sending muddy water up to 1.5 meters (5 feet) deep into more residential and commercial areas, said Agus Wibowo, the National Disaster Mitigation Agency's spokesman.

The heavy downpour that hit the capital on Sunday [23 February] had submerged the state-run Cipto Mangunkusumo hospital, the country's largest hospital, damaging medical machines and equipment, Wibowo said.

Wibowo said the floods on Tuesday [25 February] inundated scores of districts and left more than 300 people homeless, forced authorities to cut off electricity and paralyzed transportation, including commuter lines, as floodwaters reached as high as 1.5 meters (5 feet) in places.

Analyst Comment: Two tropical cyclones hit the coast of Indonesia, causing, in part, the resent flooding. However, the Indonesian capital of Jakarta has been suffering from the long-term effects of uncontrolled extraction of groundwater. The city, home to 10 million people, is rapidly sinking, and both earthquakes and flooding are a common occurrence. President Joko Widodo has ordered the relocation of capital to Borneo island.

Last month, severe flooding and landslides that hit greater Jakarta early last month killed more than 60 people, displaced hundreds of thousands and forced an airport to close. These floods were the deadliest to hit the city in more than a decade. Seasonal downpours cause dozens of landslides and flash floods each year in Indonesia. In addition to potential structural damage and loss of life, such massive flooding can trigger local evacuations, mass migration, and the spreading of waterborne diseases.

Source: https://apnews.com/72f6c4f9bece586998035b770dfbcd77

California Dam Drained for Repairs – *Accidental Events*

Excerpt: As California experiences a potentially record-breaking dry February, federal regulators have ordered that a large reservoir south of San Jose be drained due to fears a dam could collapse in an earthquake, sending a torrent of water into Silicon Valley.

The Federal Energy Regulatory Commission ordered last week [22 February] that the Anderson Reservoir be completely drained by Oct. 1 due to fears the 240-foot high earthen Anderson Dam poses too great a risk of collapse if a large earthquake strikes.

Since 2009, the dam's water level has been kept at a maximum of 74 percent of capacity because of an assessment that it could fail in a 7.2 magnitude quake or stronger. The reservoir is built along the Calaveras Fault. On Monday [24 February], amid the threat of another drought in California, Anderson Reservoir was just 29 percent full.

Analyst Comment: In 2017, the state classified the Anderson Reservoir Dam as being an "extremely high" downstream hazard. This dam is just one of approximately 14,000 in the United States that pose a significant hazard to life and property if failure occurs. More than a third of the country's dams are 50 or more years old. There are also about 2,000 unsafe dams in the United States, located in almost every state.

If a dam collapses, due to age, poor construction, erosion, a major earthquake, or some other reason, it results in a significant flash flooding event. Dam failures are generally rare but can result in serious damages and loss of life. These flash floods can have severe impacts on the environment, local wildlife, structures in the path of the water flow, and, potentially, individuals present in the area.

In 2019, a video depicting a worst-case scenario if a filled-to-capacity Anderson Dam failed in the event of a major earthquake showed major flooding in Coyote Creek that stretched all the way to San Jose. Coyote Creek flows from the dam through downtown San Jose to San Francisco Bay.

Source: https://www.foxnews.com/us/california-anderson-dam-drain-earthquake-fear-collapse-risk-santa-clara

Oil Warehouse Fire in India – *Accidental Events*

Excerpt: The residents of Madhavaram were in for a shock on Saturday evening [29 February] when they heard a thundering explosion from an oil warehouse (edible oil godown) located in the area.

Fortunately, no casualty or injury was reported. The place, located just a few metres away from the 100 feet road, caused breathing issues for the commuters who were taking the route.

The Madhavaram depot road leading to the 100 feet road was blocked for traffic and vehicles were diverted through Retteri.

The raging fire and black smoke could be spotted from even 200 metres far away due to its intensity. The reason for the fire hadn't been found yet as fire tenders and personnel were still at work.

Analyst Comment: It has been reported that the warehouse that caught fire stored oil-based products. Fire officials say the warehouse had a large amount of dimethyl sulfoxide that is used in the pharma industry. The chemicals used in the warehouse resulted in an intense fire that completely gutted the building. For days following the fire, smoke rose from the building's remains. During the fire and in the following days, higher pollution levels were detected in the area, specifically an increase in PM2.5 and PM10 particulate matter in the air. Locals appear to lack any protection from the air pollution.

This fire has again brought to attention the lack of safety measures employed in such warehouses where chemicals are stored. Structural fires that occur in HAZMAT facilities are dangerous not only during the fire, when intense heat, smoke and potential explosive incidents can occur, but also following the fire, when residents suffer the repercussions of HAZMAT materials being burned, spilled, or otherwise released into the community.

Source: https://www.newindianexpress.com/cities/chennai/2020/feb/29/massive-fire-breaks-out-in-chennais-madhavaram-no-casualties-reported-2110334.html

Pentagon Awards Contracts for Mobile Nuclear Reactor – *Accidental Events*

Excerpt: The Pentagon issued three contracts to start design work on mobile, small nuclear reactors, as part of a two-step plan towards achieving nuclear power for American forces at home and abroad.

The department awarded contracts to BWX Technologies, Inc. of Virginia, for $13.5 million; Westinghouse Government Services of Washington, D.C. for $11.9 million; and X-energy, LLC of Maryland, for $14.3 million, to begin a two-year engineering design competition for a small nuclear microreactor designed to potentially be forward deployed with forces outside the continental United States.

The combined $39.7 million in contracts are from "Project Pele," a project run through the Strategic Capabilities Office (SCO), located within the department's research and engineering side. The prototype is looking at a 1-5 megawatt (MWe) power range. The Department of Energy has been supporting the project at its Idaho National Laboratory.

Pele "involves the development of a safe, mobile and advanced nuclear microreactor to support a variety of Department of Defense missions such as generating power for remote operating bases," said Lt. Col. Robert Carver, a department spokesman. "After a two-year design-maturation period, one of the companies funded to begin design work may be selected to build and demonstrate a prototype."

Analyst Comment: The contract awards represent an initial step toward the development of mobile nuclear reactors that can be utilized in forward-deployed OCONUS locations. Per a DoD press release, the reactors can be used for defense-related purposes, in addition to civilian applications, such as disaster response work and support to critical infrastructure like hospitals.

These reactors will be designed to be deployed to a variety of locations, which may be susceptible to a wide variety of hazards to include earthquakes, tsunamis, hurricanes, and tornadoes, potentially complicating safety planning efforts. Open source reporting also indicates that the Pele reactor is intended to be deployable by road, rail, aircraft, or sea, which would require the consideration of potential radiological incidents involving transportation mishaps.

In addition to potential safety concerns, these reactors may also be appealing targets for adversaries such as terrorist groups, foreign intelligence entities, and foreign nation-state militaries.

Source: https://www.defensenews.com/smr/nuclear-arsenal/2020/03/09/pentagon-to-award-mobile-nuclear-reactor-contracts-this-week/