



Open Source Update: January 2023

**Intelligence & Analysis Division
Open Source Update**

January 2023

www.RMCGlobal.com

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	Page
Status of Investigation into U.S. Navy Bribery Scandal and the “Fat Leonard” Apprehension <i>Insider Threat</i>	2
North Korea Escalates Nuclear Threat Against South Korea <i>Foreign Nation-State Military</i>	3
Former Army Pilot Sentenced for Acting as an Agent for China <i>Foreign Intelligence Entities</i>	4
“Hack Now, Decrypt Later” Attacks Pose Risks due to Quantum Computing <i>Cyber</i>	5
China-Made Drones Intrude into D.C Airspace <i>Unmanned Aircraft-Unmanned Aircraft Systems (UA-UAS)</i>	5
Attacks on U.S. Electrical Infrastructure <i>Terrorism</i>	7
Al-Shabaab’s Threat to Eastern Africa <i>Terrorism</i>	8
Two Americans Charged for Plotting to Smuggle Military Equipment and Technology into Russia <i>Property Crime</i>	9

Hazards	Page
Storm Systems Across California Trigger Geological Hazards <i>Natural Hazards (Geological)</i>	11
New York National Guard Soldiers, Airmen Respond to Christmas Eve Snowstorm in Western New York <i>Natural Hazards (Meteorological)</i>	12
Marine Recruit’s Heat-Related Death Results in Charges <i>Natural Hazards (Meteorological)</i>	13
U.S. Navy Reports Water Contamination on Aircraft Carriers <i>Natural Hazards (Biological)</i>	14
Federal Agents to Assist Navy Investigation into Ship Fire <i>Accidental Events (Human or Technologically Caused)</i>	16
GAO Finds DoD Aircraft Mission Capable Goals Were Not Achieved <i>Accidental Events (Human or Technologically Caused)</i>	17
On The Radar	19

Threats

Status of Investigation into U.S. Navy Bribery Scandal and the “Fat Leonard” Apprehension – *Insider Threat*

Summary

As early as February 2006 until the present, the U.S. Navy and federal prosecutors have been investigating and compiling evidence regarding a wide-ranging bribery scandal involving defense contractor Leonard “Fat Leonard” Francis and the ship support contractor Glenn Defense Marine Asia (GDMA), a Thai subsidiary of the Glenn Marine Group. Francis, the company's chief executive, president, and chairman, allegedly bribed several officers within the U.S. Seventh Fleet with a half million dollars in cash, plus travel expenses, luxury items, and prostitutes, in return for information about ship and submarine movements. It was also reported he sought information about active law enforcement investigations into the company GDMA, in which he held a high leadership position.

Some open source reporting has indicated Francis may have exploited troop movement information for illicit gain by utilizing inside sources to redirect aircraft carriers, ships, and submarines to ports he controlled in Southeast Asia, gaining profits from the Navy for goods and services such as fuel, tugboats, barges, food, water and sewage removal.

Francis was also suffering health problems during the investigation, and was granted a medical furlough. This allowed him to stay at a private residence owned by one of his physicians while under 24-hour surveillance. On 04 September 2022, he escaped by cutting off his ankle monitor and fleeing to Venezuela. He was apprehended there 17 days later while preparing to leave for Russia.

Analyst Comment

Currently, U.S. federal prosecutors have filed 33 criminal charges against persons connected to bribery scandal. Concerning these charges, 22 have pled guilty while nine (9) others are awaiting trial.

Insider threats have negatively affected the U.S. Government and Department of Defense (DoD). In the past, damage by insider threats to national security has been severe, including those by defense contractors committing theft and fraud. The “Fat Leonard” arrest and Francis’s escape are part of an ongoing investigation. The follow-on prosecution for corruption within the U.S. Navy will continue as the damage from Francis’s actions are further analyzed.

Sources

<https://www.navytimes.com/news/your-navy/2022/12/29/new-in-2023-the-fate-of-fat-leonard/>

<https://www.navytimes.com/news/your-navy/2022/09/26/fat-leonard-fugitive-in-navy-bribery-case-seeks-venezuelan-asylum/>

<https://news.usni.org/2017/03/16/timeline-fat-leonard-case>

<https://news.usni.org/2022/09/22/interpol-fat-leonard-arrested-in-venezuela-trying-to-flee-to-russia>

North Korea Escalates Nuclear Threat Against South Korea – Foreign Nation-State Military

Summary

From 27 December through 31 December 2022, the Workers' Party of Korea held a five (5) day meeting in Pyongyang, North Korea in which Kim Jong-un pledged to expand North Korea's nuclear capabilities against South Korea. Kim Jong-un additionally ordered his government to "develop another ICBM system whose main mission is quick nuclear counterstrike." Furthermore, Kim Jong-un called for the mass production of short-range nuclear missiles that can be used against South Korea in addition to the production of a new intercontinental ballistic missile (ICBM) that can target the U.S. Shortly after the meeting in Pyongyang, Kim Jong-un demonstrated his determination by firing a short-range ballistic missile on 01 January in addition to launching three (3) similar short range ballistic missiles on 31 December. Kim Jong-Un stated that these missiles can deliver nuclear warheads anywhere in South Korea. Kim's commitment to expanding North Korea's nuclear capabilities has not gone unnoticed over the course of the past year. North Korea launched more missiles in 2022 (at least 95) than in any previous year, including the Hwasong-17 in November, which is the country's newest and most powerful ICBM.

Analyst Comment

In May 2022, South Korea inaugurated their new leader, Yoon Suk Yeol. Since then, Pyongyang and Seoul have engaged in both political and military conflict in which Mr. Yoon has called North Korea its "principal enemy". Moon Jae-in, South Korea's prior leader, took a different approach as he sought to reduce tensions. In 2018, North and South Korea agreed to a resolution that prohibited all military hostilities. However, since May 2022, both nations have engaged in military drills, sent UAVs over borders, and conducted dozens of missile tests. South Korea has promised to act swiftly should North Korea target it with nuclear missiles.

With Kim Jong-un emphasizing the production of nuclear weapons in 2023, North Korea may continue to enhance its capabilities in the region and, potentially, expand to other regions, despite sanctions from abroad. Increased production of nuclear weapons and other military advancements pose the most direct threat to South Korea, which is host to several DoD installations. Kim Jong-un's emphasis on labeling South Korea as the North's "undoubted enemy" has influenced Seoul's defensive strategy and operations as tensions continue to escalate. Yoon Suk Yeol has recently called for additional security cooperation with the U.S. and Japan. Seoul likely wants to counter the threat posed by Pyongyang and prevent a potentially dangerous military miscalculation that could ignite a wider conflict in the region.

Sources

<https://www.nytimes.com/2023/01/01/world/asia/north-korea-nuclear-escalate.html>

<https://www.vox.com/2023/1/7/23539605/north-korea-nuclear-kim-jong-un-united-states-south-korea>

<https://apnews.com/article/politics-south-korea-north-japan-united-states-government-06eda2aee0a8b33c30419251e06cd69f>

Former Army Pilot Sentenced for Acting as an Agent for China –

Foreign Intelligence Entities

Summary

On 07 November 2022, a former U.S. Army helicopter pilot was sentenced to 20 months in federal prison after he pled guilty to acting as an agent for China, accepting thousands of dollars from representatives of Beijing to provide aviation-related intelligence. He was employed by a defense contractor and had access to classified materials. He communicated with Chinese agents and provided them with a flash drive that contained proprietary information from his employer, which included sensitive information about aircraft that were both designed and manufactured in the U.S. In 2016, he was recruited via a technical services company from China called “LinkTek Technical Services” that worked for the government. In addition to working as an agent, he falsified his security clearance application, denying any interaction with foreign nationals, foreign businesses, and government contacts.

Analyst Comment

The Chinese government and other foreign adversaries continue to seek to gather sensitive and classified information from the U.S. government, the military, critical infrastructure, technology, and academia. Employees in those sectors are a significant target for foreign intelligence services (particularly employees that have access to classified information that can be leveraged to undermine U.S. interests and create a competitive advantage in the private sector). The U.S. government and the intelligence community are aware of China’s espionage tactics, including its talent recruitment programs. Both have enhanced security within their respective various agencies to mitigate the risk of foreign espionage. However, adversarial governments will continue to advance their technological and military capabilities by recruiting U.S. citizens.

Sources

<https://www.navytimes.com/news/2022/11/08/former-army-helicopter-pilot-sentenced-for-spying-for-china/>

<https://www.justice.gov/usao-sdca/pr/former-us-military-pilot-sentenced-acting-paid-agent-china-and-lying-national-security>

“Hack Now, Decrypt Later” Attacks Pose Risks due to Quantum Computing – Cyber

Summary

Cybersecurity experts warn that quantum computing, although not expected to be widespread for at least the next decade, poses an immediate and significant cyber risk. Quantum computers can execute complex tasks faster than traditional binary bit computers. As a result, they will likely be far more skilled at decrypting sensitive information that was encrypted by the computers of today. In anticipation of quantum decryption technology, threat actors have begun launching “hack now, decrypt later” (HN DL) attacks, wherein they steal encrypted information and store it until quantum decryption technology improves. Experts vary in their estimates of when the quantum computing threat will arrive, but most estimate between five (5) and 15 years, meaning that, although threat actors operating with current methods may not be able to access the information, they may be able to do so in the future

Analyst Comment

As quantum computing is extremely expensive, the likeliest threat actors for the foreseeable future are not hacktivists or small-scale cyber actors, but nation-state adversaries that can afford to invest in the technology and have more to gain from decrypting classified information. This is especially true if the encrypted information is still operationally relevant. Encryption is among the strongest defenses the private sector and the federal government can use to protect proprietary information and state secrets. This has created a race between cryptography experts and adversaries for quantum computing dominance. However, cryptography is just a part of an overall cyber defense strategy. In the case of HN DL attacks, social engineering attacks and insider threats that can undermine even the best security architecture. Cybersecurity education within the private sector workforce and DoD personnel remains critical.

Sources

<https://www.cpomagazine.com/cyber-security/quantum-computing-attacks-still-years-off-but-hack-now-decrypt-later-presents-immediate-cyber-risk/>

<https://www.technologyreview.com/2021/11/03/1039171/hackers-quantum-computers-us-homeland-security-cryptography/>

China-Made Drones Intrude into D.C. Airspace –

Unmanned Aircraft-Unmanned Aircraft Systems (UA-UAS)

Summary

Hundreds of drones made by the China-based company DJI, which supplies over 70% of the world’s recreational drones, have been detected flying in the Washington, D.C., area in recent months. Further, DJI drones have been altered by users to fly in restricted D.C. airspace, which has alarmed national security agencies and raised concerns of foreign espionage.

Officials do not believe that the drones have been directed by the Chinese government. However, DJI has received funding from government-owned investment entities, causing alarm among federal and private sector security professionals. Though the company claims to have no control over its drones after the items are sold, drones have been hacked to remove their internal flight restrictions. They could serve as an intelligence collection tool for malicious actors. This, along with the company's financial ties to the PRC, resulted in the Pentagon blacklisting DJI drones in 2017.

Analyst Comment

When the Pentagon banned DJI and other China-made drones, the decision was based on the assessment that DJI was considered a "Chinese military company," as DJI's drone technologies are designed in a manner that may also support the People's Liberation Army's objectives in accordance with its military-civil fusion strategy (CMF). The CMF is a national strategy of the Chinese Communist Party, and a key component of the Chinese military's modernization goals that removes the barriers between civilian research and the private sector and China's military.

DJI's connection with the Chinese government may provide the opportunity to use its technology and the otherwise recreational activity of its consumers to support the Chinese military and intelligence apparatus. The concerns with DJI drones, especially as they violate no-fly zones in the National Capital Region (NCR), mirror U.S. lawmakers' and security officials' concerns with the popular social media platform TikTok, which is owned by the Chinese company ByteDance. Over the last few years, TikTok has become a source of concern for both government and private sector security experts due to its potential to collect American citizens' private data, along with its ability to spread misinformation. As with any Chinese company, the CMF allows the Chinese government, military, and intelligence services to leverage the private sector to achieve their objectives.

DJI implemented geofencing of its drones in locations within the NCR in 2015, and there is no definitive proof that the Chinese government is directing drone incursions into prohibited areas. However, the data collected by civilians who have "jailbroken" their DJI drones may still have the potential to collect valuable information for one of the most prominent geopolitical rivals of the U.S.

Sources

<https://www.businessinsider.com/china-made-drones-flying-restricted-dc-air-space-spark-spying-fears-2022-11>

<https://2017-2021.state.gov/military-civil-fusion/index.html>

<https://www.cnet.com/news/tiktok-called-a-national-security-threat-heres-what-you-need-to-know/>

<https://americanmilitarynews.com/2022/11/hundreds-of-chinese-drones-flying-over-dc-restricted-air-space/>

Attacks on U.S. Electrical Infrastructure – Terrorism

Summary

Multiple reported threats to electrical infrastructure are under investigation after attacks on substations in North Carolina, Oregon, and Washington left thousands of customers without power during plummeting temperatures this winter.

In late November 2022, at least six (6) attacks at electricity substations in Oregon and Washington were reported to the FBI. Shortly after, in Moore County, North Carolina, two (2) substations were attacked with gunfire in early December, causing extensive damage and a five-day power outage during a cold front. Moore County is home to some personnel and their families stationed at Fort Bragg. Having studied the attack for almost a month, investigators have not yet publicly identified a suspect, but they have identified two (2) possible motives, both tied to extremist behavior. Law enforcement have yet to find evidence connecting the attack to a “drag” event scheduled to occur the night of the shooting, but the timing of the events is being considered, given the growing tensions nationwide around similar LGBTQ+ events. The second possible motive follows the recent increase in anti-government groups using online forums to urge followers to attack critical infrastructure, including the power grid. Popular posts on the topic include instructions outlining infrastructure vulnerabilities and suggesting the use of high-powered rifles, which were used in the Moore County attacks.

On 30 November 2022, shortly after the U.S. Pacific Northwest attacks and shortly before the Moore County attacks, the Department of Homeland Security (DHS) renewed a national bulletin warning that individual offenders and small organizations covering a range of extremist ideological beliefs continue to pose a threat.

Analyst Comment

Extremists have discussed and executed attacks on the U.S. power grid for some time, with a notable increase in 2020, when a 14-page document detailing how to best execute anti-government attacks circulated online.

Though the Moore County attack is still under investigation, it serves as an example of the consequences of attacks on critical infrastructure. In this case, 30,000 people, many of whom were active-duty military personnel, DoD civilians, and contractors, were left without power for almost a week during a cold front. Fort Bragg’s operations were impacted as personnel required accommodations for childcare, food security, housing, and transportation as schools closed, homes lost power, and gas stations struggled.

A similar attack in the Tacoma, Washington area occurred less than a month after the Moore County attacks, further indicating that attacks on power infrastructure may be increasing in frequency. Like Moore County, the Tacoma incident included attacks on multiple substations. There were four (4) attacks, in this case, that impacted over 1,000 customers on 25 December 2022. The impacted area is located in proximity to Joint Base Lewis-McChord, which is among the largest military installations in the country.

The electrical grid and other critical infrastructure present an attractive target for anti-government extremists. Creating mass blackouts impedes basic governmental functions from the local to federal levels, while also potentially impacting U.S. military operations. Both of these serve accelerationist extremists' goal to expedite societal collapse and/or bring about civil war.

Sources

<https://www.cnn.com/2022/12/08/us/power-outage-moore-county-investigation-thursday/index.html>

<https://www.cnn.com/2022/12/05/us/us-power-grid-attack-north-carolina-extremist-terrorism/index.html>

<https://www.cnn.com/2022/12/07/us/power-outage-moore-county-investigation-wednesday/index.html>

<https://www.nbcnews.com/news/us-news/three-substations-attacked-washington-state-rcna63214>

Al-Shabaab's Threat to Eastern Africa – Terrorism

Summary

Despite the U.S. Africa Command's (AFRICOM) efforts to contain terrorism within the continent, open source research indicates that militant Islamist violence in Eastern Africa has increased by 300% over the last decade. According to the Africa Center for Strategic Studies, as of October 2022, terrorist groups in the region were responsible for more than 6,200 violent events in 2022, a 21% increase from 2021. Furthermore, terrorist-related activity resulted in approximately 15,000 deaths in 2022, a nearly 50% increase since 2019. Open source research indicates that about 95% of the increase in militant Islamist violence comes from the western Sahel and Somalia, two (2) areas hosting U.S. personnel. The primary military Islamist threats in the region include al-Shabaab, which AFRICOM describes as "the largest and most deadly al-Qaeda network in the world." As a result, AFRICOM, which currently has about 6,000 troops in Africa, has engaged in special operations exercises with African partners and allied nations to address the security threats in the region.

Recent counterterrorism operations in Somalia also highlight the U.S.'s mission to disrupt Islamist extremism in Eastern Africa. On 01 October 2022, U.S. forces collaborated with the Somali National Army to take out Abdullahi Nadir, who was considered "one of the most important members of al-Shabaab." Furthermore, on 09 November 2022, at the request of the Somali government, the U.S. military killed 17 members of al-Shabaab in an airstrike in Somalia. Most recently, on 23 December 2022, AFRICOM conducted a self-defense strike that killed six (6) al-Shabaab terrorists in Somalia. As of mid-November 2022, the United Nations disclosed that at least 613 civilians had been killed and 948 injured in Somalia

primarily due to al-Shabaab's violence. The UN reports that most of these casualties have resulted from Improvised Explosive Device (IED) attacks by al-Shabaab extremists.

Analyst Comment

Increased militant Islamist violence, especially from al-Shabaab, could threaten the security of DoD personnel and operations of U.S. forces in Eastern Africa region. In addition to Somalia, al-Shabaab has engaged in terrorist attacks in Djibouti, a nation home to the only permanent U.S. base in Africa. In 2014, al-Shabaab claimed responsibility for a suicide attack on a restaurant in Djibouti, which resulted in one (1) fatality and approximately 20 injuries. The group announced they attacked the restaurant because it attracted "French crusaders and their NATO allies." As a result of the 2014 attack, U.S. military personnel at Camp Lemonnier were temporarily restricted to the base. In 2021, two (2) weeks before Djibouti's presidential election, al-Shabaab's leader advocated for attacks on U.S. and French interests there, as he accused the nation's president of turning the county "into a military base from where every war against the Muslims in East Africa is planned and executed." As highlighted by the self-defense strike against al-Shabaab on 23 December 2022, the U.S. military continues to have a presence in the region and supports local forces fighting al-Shabaab.

Sources

<https://www.militarytimes.com/news/your-military/2022/10/19/pentagon-says-terror-attacks-in-africa-grew-by-300-over-last-decade/>

<https://africacenter.org/spotlight/sahel-and-somalia-drive-uninterrupted-rise-in-african-militant-islamist-group-violence-over-past-decade/>

<https://www.africanews.com/2021/03/29/al-shabaab-calls-for-attacks-on-u-s-french-interests-in-djibouti/>

<https://www.cnn.com/2022/11/11/politics/us-airstrike-somalia-al-shabaab/index.html>

<https://www.africom.mil/pressrelease/35066/somali-forces-engage-al-shabaab-insurgents>

<https://www.stripes.com/djibouti-based-troops-restricted-to-base-following-bombing-1.285636>

Two Americans Charged for Plotting to Smuggle Military Equipment and Technology into Russia – Property Crime

Summary

In December 2022, two (2) Americans and five (5) Russian nationals were charged for plotting to smuggle military equipment into Russia. According to the U.S. Department of Justice (DOJ), some of this technology was allegedly found on battlefields in Ukraine. The seven (7) individuals "unlawfully purchased and exported highly sensitive and heavily regulated electronic components" as part of a money laundering scheme. The equipment included dual-use technologies from U.S. companies in addition to sniper rifle ammunition.

The technology and equipment in question could assist in the development of “nuclear and hypersonic weapons, quantum computing and other military applications” according to the DOJ. The individuals have been charged with conspiracy to violate the Export Control reform Act (ECRA), smuggling, and failure to comply with the Automated Export System in relation to the transportation and distribution of electronics.

Analyst Comment

The two (2) Americans charged attempted to bolster the Russian military’s war efforts in Ukraine. Illegally transferring weapons and dual use-technology across borders and seas not only enhances adversaries’ capabilities but supports transnational criminal activity. Transnational criminal organizations may conspire with Americans to participate in smuggling or other illegal activity on behalf of foreign governments. American military equipment and technology can be used in fighter aircraft, ballistic and hypersonic missile systems, smart munitions, and other military applications. While transnational criminal organizations will always search for ways to illegally acquire this equipment, they sometimes target servicemembers or veterans who have access to equipment, technology, and other resources. Personnel stationed on installations overseas may pose an enhanced insider threat if they cooperate with these groups for personal gain.

Sources

<https://www.navytimes.com/news/your-military/2022/12/14/7-charged-in-scheme-to-smuggle-military-equipment-to-russia/>

<https://www.cnn.com/2022/12/13/politics/russian-and-us-nationals-smuggling-ammo-russian-military-fsb/index.html>

<https://www.justice.gov/opa/pr/russian-military-and-intelligence-agencies-procurement-network-indicted-brooklyn-federal>

<https://www.reuters.com/world/us-prosecutors-charge-five-russians-pdvsa-traders-with-sanctions-evasion-2022-10-19/>

Hazards

Storm Systems Across California Trigger Geological Hazards –

Natural Hazards (Geological)

Summary

Landslides of rock and mud closed roadways across California during heavy rains at the start of the year. There were downpours and flooding across much of the state and multiple feet of snow in the Sierra Nevada. The atmospheric river storm, a long and wide plume of moisture pulled in from the Pacific Ocean, affected the northern part of the state beginning on 30 December 2022. A winter storm warning was in effect into 01 January 2023 for the upper elevations of the Sierra from south of Yosemite National Park to north of Lake Tahoe, where as much as five (5) feet of snow was expected atop the mountains. A flood watch was in effect across much of Northern California through New Year's Eve. Officials warned that rivers and streams could overflow and urged residents to prepare with sandbags.

As of 30 December, landslides already had closed routes in the San Francisco Bay Area, between Fremont and Sunol, as well as in Mendocino County near the unincorporated community of Piercy and in the Mendocino National Forest.

Analyst Comment

For the last two (2) months California has been experiencing extreme weather systems bringing heavy rain, flooding, hail, lightning, and landslides. Millions of residents have received flood warnings, and nearly 50,000 people were under evacuation orders. Heavy rain and flooding contribute to erosion, increasing the chances of landslides occurring in the same region. Rockslides and mudflows, both types of landslides, have also been seen. Furthermore, coastal areas have been made more vulnerable to landslide occurrences due to rising sea levels. At least 17 deaths have occurred as a result of these storm systems. The current storm system was projected to continue until 17 January. Further geological and economic impacts were and are expected.

While the rain may come as a relief to drought-stricken California, much more precipitation is needed to make a significant difference. The past three (3) years have been California's driest on record. The entirety of the state is in a D1 drought conditions or above. The state has noted the water content in the snowpack is more than double the average, easing short term drought concerns.

Sources

<https://www.cnn.com/2022/12/10/us/california-landslide-palos-verdes-estates/index.html>

<https://apnews.com/article/floods-weather-natural-disasters-landslides-and-mudslides-storms-21b103e791710f4af6ca0ce45c6030b5>

<https://abcnews.go.com/Sports/wireStory/storm-brings-flooding-landslides-california-96000459>

<https://droughtmonitor.unl.edu/CurrentMap.aspx>

New York National Guard Soldiers, Airmen Respond to Christmas Eve Snowstorm in Western New York –

Natural Hazards (Meteorological)

Summary

Open source reporting indicates that 849 New York National Guard Soldiers and Airmen participated in a week-long mission following a snowstorm in the Buffalo area starting on 24 December 2022. According to the National Weather Service, areas in western New York received at least 50 inches of snow. While the governor declared a state of emergency ahead of the storm's arrival and initially tasked approximately 50 National Guard Soldiers and Airmen, additional personnel were required after the storm hit. By 29 December 2022, the number of troops reached its height at 701. Using a total of 172 deployed vehicles and four (4) trailers, Soldiers and Airmen rescued 124 people from stranded cars, moved 264 medical personnel, transported 77 patients, visited 3,755 households for health and welfare checks, established nine (9) traffic control points, plowed six (6) miles of roads, and cleared 8.5 acres of parking. While executing this mission, the New York National Guard also had 700 personnel on state active duty in New York City assisting with the influx of migrants and another 700 personnel in the city as part of the Joint Task Force Empire Shield security mission.

According to weather reports, the storm started as a rain event in Buffalo on 23 December 2022. The 1.98 inches of precipitation in Buffalo on 23 December broke the prior daily record of rain that had stood since 1878. After the heavy precipitation event, arctic air rushed in and turned the rain into snow on the morning of the 23rd. Reporting also suggests that a "bomb cyclone" primarily generated the winter storm event. A "bomb cyclone" is a mid-latitude storm whose central air pressure falls at a rate of one (1) millibar per hour for at least 24 hours, typically taking the form of nor'easters along the Eastern Seaboard. The "bomb cyclone" over Christmas weekend in Buffalo was particularly strong because of the arrival of an exceptionally cold air mass and the rapid strengthening of a low-pressure zone at high altitudes over the Upper Midwest. Furthermore, the storm's slow movement prolonged the blizzard conditions of high wind and heavy snow in western New York. Ultimately, 39 people in the Buffalo area had died by the time the snowstorm was over.

Analyst Comment

Buffalo, located next to Lake Erie, is among the snowiest cities in the U.S. since the area is prone to lake-effect snow. This form of snow occurs anywhere from a few minutes to several days when cold, dry arctic air passes over a large, relatively mild lake, resulting in narrow bands of clouds. According to some climate experts, climate change could increase the potential for extreme rain and snow events, including in the Buffalo area. According to NOAA's 2022 climate summary for New York, the state's temperatures have risen 2.5 degrees Fahrenheit since the start of the 20th century. Warming temperatures could increase the time it takes for the Great Lakes to freeze over in the fall and winter, potentially intensifying lake-effect snow events in the region.

Heavy snow events and winter storms could impact the missions of DOD installations, damage facilities, and affect personnel schedules. Snowstorms, such as the Buffalo storm, could result in roadway closures and other transportation challenges, potentially limiting accessibility to DoD facilities, delaying the arrival of critical equipment and other goods, and requiring the mobilization of personnel. Also, fatalities, injuries, and damage to the surrounding area of an installation could strain resources and require increased personnel response.

Sources

https://www.army.mil/article/263062/ny_national_guard_mobilized_849_for_deadly_buffalo_blizzard_response

<https://www.navytimes.com/news/your-military/2022/12/28/new-york-national-guard-deploys-to-assist-with-deadly-snowstorm/>

<https://www.dvidshub.net/news/435904/ny-national-guard-deploys-christmas-snow-storm-response>

<https://www.accuweather.com/en/winter-weather/deadly-lake-effect-blizzard-buries-buffalo-in-over-4-feet-of-snow/1429773>

<https://www.washingtonpost.com/weather/2022/12/21/bomb-cyclone-explained/>

<https://www.msn.com/en-us/weather/topstories/the-buffalo-storm-exploded-into-a-meteorological-bomb-here-s-why/ar-AA15KEgj?cvid=c5501875b6414618b56d751f6aa34796#image=4>

<https://www.msn.com/en-us/weather/topstories/buffalo-death-toll-rises-making-snow-storm-deadliest-in-more-than-4-decades-military-police-enforces-driving-ban/ar-AA15I2Uw>

<https://www.msn.com/en-us/weather/topstories/climate-change-wont-make-winter-storms-and-blizzards-go-away-scientists-explain-why/ar-AA15IYth>

Marine Recruit's Heat-Related Death Results in Charges –

Natural Hazards (Meteorological)

Summary

Marine Staff Sgt. Steven T. Smiley, a drill instructor at MCRD Parris Island, South Carolina, has been charged with negligent homicide and related offenses under the Uniform Code of Military Justice (UCMJ) for the death of Pfc. Dalton Beals, 19, on 04 June 2021.

Beals died during the Crucible event that occurs near the end of recruit training at Parris Island. His cause of death was determined to be hyperthermia, commonly known as overheating. A subsequent investigation faulted Smiley for not properly supervising Beals

and other recruits and making them do extra physical training even though the temperature was in the 90s that day.

Analyst Comment

Heat is the leading cause of weather-related deaths in the U.S. Strenuous physical activity or simply prolonged exposure in high heat conditions can lead to heat related illness. This includes heat cramps, heat exhaustion, and heat stroke.

It is important to understand the difference between temperature and apparent temperature, known more commonly as the heat index. The higher the heat index, the greater the likelihood of heat disorder occurrence. The heat index is calculated utilizing air temperature and relative humidity. Relative humidity plays a key role in the body's ability to regulate temperature. When a body becomes too hot, it will begin to sweat. The sweat then evaporates, cooling the body. However, the higher the humidity, the slower the rate of evaporation. Therefore a 90°F day with high humidity is much more dangerous than a day with the same temperature and low humidity.

A key consideration when using heat index values is noting that the value is intended to reflect apparent temperature in shady locations. The same temperature and humidity can see up to a 15°F heat index increase in direct sunlight. Failing to account for the heat index and the condition of personnel during training, particularly recruits, can result in both injuries and death.

Sources

<https://taskandpurpose.com/news/marine-corps-drill-instructor-charged-recruit-death-parris-island/>

<https://www.weather.gov/ama/heatindex>

<https://www.noaa.gov/stories/excessive-heat-silent-killer>

<https://www.noaa.gov/media-advisory/extreme-heat-media-resource-guide>

<https://www.livescience.com/what-is-relative-humidity>

U.S. Navy Reports Water Contamination on Aircraft Carriers –

Natural Hazards (Biological)

Summary

On 13 October 2022, the U.S. Navy announced that it had found Escherichia coli (E. coli) bacteria in the drinking water of the aircraft carrier USS Abraham Lincoln. This statement came after Sailors noticed an "odor and cloudy appearance" in the ship's water on 21 September 2022. On 26 September 2022, an outside laboratory found that the water was within the standards for pH, turbidity, aluminum, copper, lead, sodium, and hardness. According to the Centers for Disease Control and Prevention, E. coli infections can be very

mild, but others can be severe. Symptoms of an infection can include stomach cramps, diarrhea, vomiting, and fever. The Navy has since confirmed no illnesses related to the contamination.

This is the second time in a few weeks that the Navy has reported contaminated water on its ships. Traces of jet propellant-5 were found in the water of the aircraft carrier USS Nimitz on 21 September 2022. This type of incident is not an isolated event. Drinking water can become contaminated with jet fuel because the two can mix in the ballast tank system used on aircraft carriers. The ballast tank systems are needed to help control buoyancy and stability on ships. Sailors aboard the aircraft carrier reported to open source news that the contamination was worse than initially indicated, and that they were not receiving adequate medical attention. The Navy stated that there were no ill effects related to jet fuel contamination and that the ship's command would continue to monitor the situation and take appropriate action to safeguard the crew.

Analyst Comment

The risk of contamination of drinking water aboard ships has always existed. Mishaps sometimes occur involving improper treatment and purification of water. The most likely source of contamination is usually volatile organic compounds, total petroleum hydrocarbons, disinfection by-products (total trihalomethanes), and lead. These contaminants can result in adverse health effects, including gastrointestinal illness and neurological damage. Exposure to high doses of chemicals can also lead to skin discoloration, organ damage, and developmental or reproductive effects. Exposure to lower doses over long periods of time can lead to chronic, long-term conditions such as cancer. Ultimately, these incidents can have a negative affect on unit and installation readiness and servicemember welfare.

Sources

<https://www.businessinsider.com/us-navy-e-coli-aircraft-carrier-uss-abraham-lincoln-water-2022-10>

<https://www.navytimes.com/news/your-navy/2022/10/12/another-aircraft-carrier-is-grappling-with-water-issues/>

<https://www.businessinsider.com/navy-jet-fuel-traces-uss-nimitz-sailor-says-worse-problem-2022-9?inline-endstory-related-recommendations=>

<https://www.usgs.gov/special-topics/water-science-school/science/bacteria-and-e-coli-water>

<https://www.cdc.gov/healthywater/drinking/contamination.html>

Federal Agents to Assist with Navy Investigation into Ship Fire – *Accidental Events (Human or Technologically Caused)*

Summary

Federal agents with the Bureau of Alcohol, Tobacco, Firearms and Explosives (ATF) are helping the U.S. Navy investigate a fire that broke out aboard the Arleigh Burke-class guided-missile destroyer USS Carney on 23 December 2022 while it was moored for maintenance. The fire was quickly extinguished by crewmembers, Jacksonville Fire and Rescue, and a team from the nearby destroyer USS Mason. This is the latest such report following a second publicly acknowledged fire incident which occurred at NAVSTA Mayport, Florida. The Navy's request of ATF support to investigate the fire will help confirm if the incident is a potential crime scene. This investigation of the incident is currently ongoing, and no determinations have been made by the Navy or the ATF.

Analyst Comment

Recently, the Navy's most destructive fires have occurred while ships are undergoing repairs in shipyards. As mentioned earlier, a fire broke out aboard the USS Milwaukee, a littoral combat ship based at NAVSTA Mayport in July 2022. That fire was quickly extinguished. However, scanner traffic suggested that four (4) Sailors had to be evaluated for smoke inhalation. The Navy later reported de-smoking the affected spaces aboard the ship and that all Navy and contractor personnel were safe and accounted for.

In July 2020, the USS Bonhomme Richard experienced a catastrophic fire while undergoing maintenance at NAVBASE San Diego, California. During the follow-on investigation, it was reported the fire suppression system was turned off at the time of the blaze for maintenance work. That fire resulted in 60 people being treated for minor injuries, as well as heat- and smoke-related complaints.

Fires can also prompt air quality advisories for surrounding areas. Individuals who have health concerns or those who smell smoke are always advised to close their windows onboard installations and to limit time outdoors (to include exercising) due to air quality concerns. There were no stated concerns from open source reporting or from the Florida Department of Environmental Protection New & Press Releases regarding the toxicity of the fumes from this recent incident. However, advisories normally relate to inhalation of particulate matter emanating from a fire.

Sources

https://www.military.com/daily-news/2022/12/28/navy-calls-atf-investigators-probe-blaze-aboard-destroyer-docked-florida.html?utm_source=sailthru&utm_medium=email&utm_campaign=mil-ebb&SToverlay=de88742f-46f7-4f2c-819d-3b36a47d6a7e

<https://www.military.com/daily-news/2022/07/29/fire-aboard-uss-milwaukee-florida-naval-base.html>

<https://www.military.com/daily-news/2021/10/20/navy-brass-doesnt-plan-major-changes-after-bonhomme-richard-fire-expects-captains-ask-help.html>

<https://www.navy.mil/Press-Office/News-Stories/Article/2816283/navy-releases-extensive-bonhomme-richard-fire-report-major-fires-review/>

<https://www.defensenews.com/naval/2022/07/05/new-details-emerge-about-the-2020-bonhomme-richard-fire-ahead-of-censure-of-three-star/>

https://floridadep.gov/news?field_is_this_a_press_release_value=All&field_division_tid_1=351

GAO Finds DoD Aircraft Mission Capable Goals Not Achieved – Accidental Events (Human or Technologically Caused)

Summary

According to a report published by the Government Accountability Office (GAO) on 10 November 2022, 26 out of the 49 types of DoD aircraft studied did not reach their annual mission capable goals in any fiscal year between FY2011-FY2021. Of the 26 aircraft that did not meet their targeted mission capable rate, which the GAO describes as the “percentage of total time when the aircraft can fly and perform at least one mission,” eight (8) were Navy airframes. Furthermore, of the 15 total Navy aircraft studied by the GAO, only two (2) aircraft met their annual mission-capable goals for at least five (5) years from FY2011-FY2021. In addition, all nine (9) of the Marine Corps aircraft studied never met their annual mission-capable goals from FY2011-FY2021. Despite the mission capability shortcomings of most of the 49 airframes, operating and support (O&S) costs of the reviewed aircraft totaled about \$54 billion in FY2020. Also, the GAO reports that the (O&S) expenses of the Navy and Marines Corps have increased throughout FY2011-FY2021.

The GAO’s analysis of selected DoD aircraft indicates that various sustainment challenges could impact mission-capable rates and increase costs to maintain aircraft. For instance, the GAO found that there have been challenges related to the age of aircraft, such as DoD airframes requiring an unexpected replacement of parts and repairs. Also, the DoD has experienced delays in acquiring replacement aircraft for certain models, and some airframes received service life extensions. Furthermore, there were maintenance issues for dozens of aircraft, as the DoD encountered delays in depot maintenance, personnel shortages, and unscheduled repairs. Lastly, the GAO identified challenges with supply support, as the DoD faced parts shortages and delays, parts obsolescence, and diminished manufacturing sources with most of the studied aircraft.

Analyst Comment

Failing to reach mission-capable goals, which are used to assess the health and readiness of aircraft fleets, could impact the missions of installations and increase the DoD’s O&S costs to maintain airframes. For instance, the grounding of Navy and Marines T-45C Goshawk training jets in October 2022 highlights the various sustainment challenges affecting some

aircraft. In October 2022, one of the Navy's T-45C Goshawk training jets experienced a "low-pressure compressor blade failure" during a preflight check, leading to the grounding of the entire fleet. Open source reporting indicates that there have been concerns with the age of the Navy's Goshawk fleet, as the average aircraft in the fleet is 20 years, and some models date back to the late 1980s.

Sustainment challenges could also lead to aircraft mishaps, potentially resulting in fatalities, injuries, and destroyed aircraft. In September 2021, two (2) individuals were injured after a Navy T-45C Goshawk jet trainer assigned to NAS Kingsville crashed near NAS JRB Fort Worth, Texas. In addition, in August 2022, a Navy T-45C Goshawk crashed while approaching NAS Kingsville. Safety standdowns resulting from aircraft mishaps could further affect the operations at installations. A delay in training schedules, installation activities, and maintenance could lead to additional challenges and impact future readiness.

Sources

<https://www.marinecorpstimes.com/news/your-air-force/2022/11/16/heres-all-the-military-planes-that-keep-falling-short-on-readiness/>

<https://www.gao.gov/assets/gao-23-106217.pdf>

<https://taskandpurpose.com/news/military-aircraft-mission-capable-rates-gao/>

<https://www.stripes.com/branches/navy/2022-10-26/navy-goshawk-engine-problem-trainer-7814701.html>

<https://www.navytimes.com/news/your-navy/2022/08/16/t-45-goshawk-crashes-near-naval-air-station-kingsville-pilot-safe/>

<https://www.navy.mil/Press-Office/Press-Releases/display-pressreleases/Article/2780932/updated-navy-t-45c-goshawk-crashes-in-lake-worth-texas-no-fatalities/>

On the Radar

- **Riots in Brazil.** *Following the accreditation of Lula da Silva's electoral victory, supporters of ex-President Jair Bolsonaro stormed the Presidential Palace, the offices of Congress, and the Supreme Court. While a majority of Brazilians polled condemn the attack, further political instability and tensions are likely to remain, with possible civil disturbance activity, violent crimes, or property crimes resulting.*
- **Development of a 100-Vessel Fleet of Unmanned Surface Ships in the Middle East.** *Open source reporting indicates that by the end of the summer, the U.S. Navy seeks to develop a 100-vessel fleet of unmanned surface ships, or drone boats, to patrol the waters of the Middle East. Over the past few months, there have been at least three (3) incidents in which the U.S. Navy accused Iran of smuggling weapons and war supplies within the region. Most recently, on 06 January 2023, a Navy patrol coast ship intercepted a fishing vessel carrying 2,116 AK-47 rifles while transiting the Gulf of Oman. According to Naval Forces Central Command, the vessel was along a maritime route from Iran to Yemen.*