Open Source Update: April 2024

Intelligence & Analysis Division
Open Source Update

April 2024

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

China's New Ten Dash Line Map – *Foreign Nation-State Military*

Summary

The 1982 United Nations Convention on the Law of the Sea created Exclusive Economic Zones (EEZ)s which generally extend 200 nautical miles beyond a nation's territorial sea. Each nation has jurisdiction over living and nonliving resources within those boundaries. In August 2023, China's Ministry of Natural Resources released an updated official map of the geographical territories claimed by the People's Republic of China (PRC). Like previous versions of the map, China made claims to over 90% of the South China Sea, including maritime regions within the Vietnamese, Malaysian, Brunei, Indonesian and Philippine EEZs. The new map placed an additional dash in the line that also encompasses the island of Taiwan.

Historically, China did not claim these areas until the Republic of China (ROC; Taiwan) made its own claim in 1947. After the ROC lost the civil war, Mao Zedong established the PRC and chose to continue the claims made in the ROC map. These claims were based on supposed ancient Chinese exploration under the Song Dynasty. However, a leaked diplomatic document from 2008 indicates that senior PRC maritime officials did not know of any documented historical basis for territorial claims to the South China Sea.

In 2016, the Philippines filed 15 allegations against China in the Permanent Court of Arbitration in the Hague. The court ruled unanimously in favor of the Philippines on almost every count. This included the dispute over Mischief Reef in the Spratly Islands, which the PRC occupied in 1995 and has now developed a military grade runway and port facilities. The court stated that the Spratly Islands fall within the Philippine EEZ. This means that China is in a state of unlawful occupation. The court also ruled that illegal fishing and environmentally damaging artificial island construction by China infringe on Philippine sovereign rights. Regardless, the PRC has constructed ports, airstrips and military installations in the Parcel, Spratly, and Woody Islands with as many as 27 outposts supporting fighter aircraft, cruise missiles, anti-aircraft missiles, and radar systems. In response, the Department of Defense (DoD) has expanded its presence and operations. All branches of the DoD have partnerships and developing infrastructure plans with the Armed Forces of the Philippines. The USMC created Marine Rotational Force Southeast Asia (MRF-SEA) which will deploy yearly to the Philippines for training exercises. Operation Cobra Gold is a yearly training exercise partnership between the U.S. Army and USMC in Thailand which is expanding in size and scope. The U.S. Navy routinely conducts Freedom of Navigation Operations in the South China Sea along with partners in the region. These operations have resulted in regular close encounters by ships and aircraft with PRC assets, including several aviation and maritime mishaps.

Analyst Comment

The PRC seeks to undermine U.S. alliances and security partnerships in the Indo-Pacific region and to leverage its growing capabilities, including its economic influence and the People's Liberation Army's (PLA) growing strength and military footprint, to coerce its neighbors and threaten their interests. The PRC's increasingly provocative rhetoric and coercive activity towards Taiwan are a product of risk miscalculation that threatens the peace and stability of the Taiwan Strait. This is part of a broader pattern of destabilizing and coercive PRC behavior that stretches across the East China Sea, the South China Sea, and along the Line of Actual Control. The PRC has expanded and modernized nearly every aspect of the PLA, with a focus on offsetting U.S. military advantages. The PRC is therefore the multi-domain pacing challenge for the DoD.

The PRC is capable of combining its economic, diplomatic, military, and technological power to mount a sustained challenge to a stable and open international system. The PLA has already fielded sophisticated weapons and platforms in every warfare domain, instituted major organizational reforms to enhance joint operations, and improved its combat readiness. As a result, it is nearing the status of a global competitor to the U.S. and is a credible peer competitor in the region. These developments, along with future capabilities, are designed to provide options for China to dissuade, deter, or, if ordered, defeat U.S. and allied intervention during a large-scale theater campaign, such as a war over Taiwan. As the DoD increases infrastructure and operations in such a contested environment, the threat posed by associated risks also increases.

Sources

https://www.bostonpoliticalreview.org/post/china-s-new-map-the-10-dash-line

https://media.defense.gov/2022/Oct/27/2003103845/-1/-1/1/2022-NATIONAL-DEFENSE-STRATEGY-NPR-MDR.PDF

https://www.dia.mil/Portals/110/Documents/SFR/DIA%202022%20ATA%20SFR.pdf

https://crsreports.congress.gov/product/pdf/IF/IF12550

Chinese National Charged in Alleged Plan to Steal Google's Artificial Intelligence Trade Secrets – *Foreign Intelligence Entities*

Summary

On 07 March 2024, the U.S. Department of Justice (DOJ) announced that a national of the People's Republic of China (PRC) and resident of Newark, California, was charged with four (4) counts of theft related to an alleged plan to steal artificial intelligence (AI) trade secrets from Google. The indictment states that the Chinese national, hired by Google in 2019, transferred over 500 files containing trade secrets and other confidential information from Google's network to his personal account two (2) years ago. Shortly before the individual started stealing the data, he was offered the Chief Technology Officer position at an early-

stage technology company in China. Also, while working for Google, he founded and served as CEO of a separate technology company in the AI and machine learning industry

Starting in late 2022, the former Google employee traveled to the PRC for several months to attend investor meetings to raise capital for his new company. Furthermore, the indictment reveals that the Chinese national allegedly permitted a coworker to use his Google-issued access badge and scan into a company building entrance while he was in the PRC in December 2023, making it appear as if he was working in the U.S. The accused could serve a maximum penalty of 10 years in prison and pay a $250,000 fine for each count following the determination of a federal district court judge.

Analyst Comment

The PRC's investment in AI systems highlights China's goals of becoming a more significant technology and military power and bolstering its malign influence and intelligence operations. According to the Office of the Director of National Intelligence's 2024 Annual Threat Assessment of the U.S. Intelligence Community, a key PRC state-owned enterprise signaled its plan to allocate at least $13.7 billion into industries including "AI, advanced semiconductors, biotechnology, and new materials." Furthermore, China announced in October 2023 a "Global AI Governance Initiative" to strengthen international support for its AI governance vision. Open-source intelligence also indicates that China is researching AI applications, such as "support for missile guidance, target detection and identification, and autonomous systems."

This indictment of the former Google employee shortly followed public remarks from DOJ and FBI officials warning of national security concerns related to AI. DOJ officials have expressed their concern that AI can accelerate the spread of disinformation and present new opportunities for hackers, citing the threat of foreign malign influence threats using generative AI in the upcoming presidential election. As China continues to rapidly develop its AI and big data analytics and experiment with generative AI, the PRC could more effectively promote pro-China narratives, counter democratic principles, and more effectively exploit societal divisions in America.

Sources

https://apnews.com/article/north-korea-weapons-program-it-workers-f3df7c120522b0581db5c0b9682ebc9b

https://www.justice.gov/opa/pr/justice-department-announces-court-authorized-action-disrupt-illicit-revenue-generation

https://www.justice.gov/opa/pr/three-north-korean-military-hackers-indicted-wide-ranging-scheme-commit-cyberattacks-and

https://www.dni.gov/files/ODNI/documents/assessments/ATA-2022-Unclassified-Report.pdf

https://www.ic3.gov/Media/Y2023/PSA231018?utm_medium=email&utm_source=govdelivery

https://apnews.com/article/north-korea-missile-launch-bc0391e981b2eedce5dc17734e27ee0c

https://apnews.com/article/north-korea-kim-party-meeting-missiles-27803fcfbfa9cb2a89d6fb5e824e9c0c

https://www.dni.gov/files/ODNI/documents/assessments/ATA-2024-Unclassified-Report.pdf

Hackers Target Sewer and Water Systems – *Cyber*

Summary

In recent history, cybercriminals have posed a threat to power grids, water, and sewage systems. Hackers have been attempting to carry out cyberattacks throughout the country that could disrupt the flow of clean drinking water. These systems are often outdated and lack the proper security due to a shortage of necessary resources, which makes them vulnerable to persistent cyberattacks.

On 18 March 2024, the Environmental Protection Agency (EPA) sent a letter to governors reporting recent cyberattacks on water systems. The EPA believed the threat actors to be affiliated with the Iranian Government Islamic Revolutionary Guard Corps (IRGC), and the People's Republic of China (PRC), which sponsors a hacker group known as Volt Typhoon, which has targeted and disrupted critical infrastructure systems in the U.S. Cyber actors affiliated with the IRGC were also able to target and disable controllers that helped analyze wastewater treatment.

Analyst Comment

Cyberattacks can disrupt the operation of water treatment and distribution systems. This can result in inconvenience for residents and businesses and pose health risks if the interruption affects access to clean water. If they are able to bypass network security, hackers can manipulate water treatment processes remotely, altering the chemical composition or introducing contaminants into the water supply. This poses significant health risks to consumers and can lead to widespread illnesses or even fatalities.

Many DoD installations rely on local water systems. If these systems are compromised, it can impact daily operations, sanitation, and even firefighting capabilities. Successful cyberattacks on critical infrastructure set dangerous precedents and may embolden adversaries to target other essential services or sectors vital to national defense.

Sources

https://www.msn.com/en-us/news/us/oregon-reviewing-water-infrastructure-security-following-cyber-attack-warning/ar-BB1kluLh

https://www.cisa.gov/news-events/alerts/2023/11/28/exploitation-unitronics-plcs-used-water-and-wastewater-systems

https://www.epa.gov/system/files/documents/2024-03/epa-apnsa-letter-to-governors_03182024.pdf
https://www.reuters.com/technology/cybersecurity/us-warns-that-hackers-are-carrying-out-disruptive-attacks-water-systems-2024-03-20/

Cyberattack Against Commercial Prescription Program Hamstrings Military Pharmacies Around the World – *Cyber*

Summary

On 23 February 2024, a cyberattack shut down the Change Healthcare prescription processing program, which is contracted by DoD healthcare systems. This disruption has impacted pharmacy operations, including manning and resources. Both retail pharmacies and pharmacies at DoD installations were affected. Change Healthcare disclosed on 21 February 2024 that the company network was compromised in the cyberattack. Change Healthcare disconnected its systems as soon as it became clear it was a cyberattack. Urgent prescriptions took priority and military pharmacies followed a manual procedure to fill prescriptions.

Analyst Comment

It has been determined that the Blackcat ransomware gang was behind the Change Healthcare cybersecurity attack. First reported on 21 February 2024, Blackcat gained access to Change Healthcare information technology systems and disrupted prescription deliveries. The event also caused delays to claim processing and hospital revenue cycle operations. Healthcare organizations were reconsidering connection or reconnection to Change Healthcare systems following mitigation efforts. Connection or reconnection to these systems can cause business and clinical disruptions to healthcare organizations. Hospitals and healthcare businesses also faced obstacles in acquiring patient care authorizations and payment delays. Pharmacy services and TRICARE experienced delays in their typical operations as well. Clinics and hospitals resorted to manual procedures or electronic workarounds to continue operations.

On 27 March, Change Healthcare's parent company, UnitedHealth Group, said it had hired a contractor to conduct a review of data that is "likely" to contain personally identifiable information (PII) and claims data. As of that announcement, there was no evidence of patient PII being published online. Change Healthcare moved forward with plans to release updated claims software to resume service. Change Healthcare's electronic payments platform were restored as of 15 March. UnitedHealth Group also restored most of Change Healthcare's pharmacy network services earlier in March.

Sources

https://www.military.com/daily-news/2024/02/23/military-patients-face-delays-filling-prescriptions-because-of-cyberattack-against-health-tech.html

https://www.militarytimes.com/pay-benefits/military-benefits/health-care/2024/02/22/cyberattack-slows-prescription-processing-at-military-pharmacies/

https://www.healthcarefinancenews.com/news/blackcat-ransomware-gang-reportedly-behind-change-cyberattack

https://healthitsecurity.com/news/change-healthcare-disconnects-system-amid-cyberattack

Haiti's Main Port Closes as Gang Violence Continues – *Gang Activity*

Summary

On 10 March 2024, U.S. Marines were sent to Haiti to evacuate non-essential personnel and support the American embassy amid ongoing gang attacks. The country's capital of Port-au-Prince remains the center of unrest. Gang violence has occurred in multiple locations around the capital and near the embassy in Tabarre, including the looting and overtaking of local businesses, a jailbreak, the theft of cargo containers and vandalism at the main seaport, taking control of police stations, and forcing the closure of international and domestic airports. Gangs in the area now control of more than 80% of the capital and demanded the resignation of Prime Minister Ariel Henry. A state of emergency and a curfew have been imposed by the Haitian government. Members of the Haitian army have been deployed to assist the country's National Police. The U.S. has aided efforts by providing additional ammunition.

Analyst Comment

The U.S. Embassy has stated that is committed to supporting the Haitian community during this period. The Embassy is working to mobilize police support, facilitate a peaceful transition of power, and advance the security mission's deployment. An emergency meeting between Caribbean leaders, the U.S., France, the U.N., Canada, and Brazil was scheduled for 11 March 2024 in Jamaica to address the ongoing violence. Since the meeting, Prime Minister Henry pledged to resign on 12 March 2024. Haiti is preparing for new leadership and attempting to create a transitional authority. However, death threats and security concerns have hindered the process of choosing a new leader. Due to the security of the members and ongoing disagreements about the legality of the process, the transition group still has not been formed.

Continued attacks may put embassy personnel in danger and require increased logistical support from the Marines, as demonstrated in evacuation efforts. In response, the State Department has decided to arrange the departure of additional embassy personnel following the first wave of evacuations. As of 17 March 2024, more than 340 U.S. citizens have departed the area from Port-au-Prince.

Sources

https://www.msn.com/en-us/news/world/us-military-flies-marines-into-haiti-embassy-evacuating-some-staff-in-overnight-airlift/ar-BB1jDi4K

https://www.usnews.com/news/world/articles/2024-03-10/us-flies-forces-in-to-beef-up-security-at-embassy-in-haiti-and-evacuate-nonessential-personnel

https://apnews.com/article/haiti-us-embassy-security-gang-violence-1b720280fa85c87ccf0768d3156dbd23

https://www.msn.com/en-us/news/world/haiti-s-main-port-closes-as-gang-violence-spirals/ar-BB1jvY7I

https://www.cnbc.com/2024/03/12/haitian-prime-minister-ariel-henry-resigns-after-jamaica-talks.html

https://www.msn.com/en-us/news/world/haitian-prime-minister-ariel-henry-to-resign/ar-BB1jJDEj

https://www.reuters.com/world/americas/haitian-leader-says-he-will-quit-after-transitional-council-formed-gang-violence-2024-03-12/

https://apnews.com/article/haiti-council-gangs-violence-442ae5ac6eeab904ceaaa23e7672e6f0

https://apnews.com/article/haiti-gangs-transitional-council-44389048f6b36109daabb81c1b356a88

https://actualnewsmagazine.com/english/haiti-the-appointment-of-transitional-authorities-is-still-awaited/

New "Zombie Drug" Spreads in West Africa – *Narcotics*

Summary

Sierra Leone, and other parts of West Africa are fighting an ongoing battle with a new drug called Kush. This drug may have the same name as one that is commonly used in the U.S., but it is much different. This Kush is a form of a synthetic cannabinoid that is cut with a number of other drugs. Due to the country's struggling economy, there is no accurate data available to depict how fast the drug is spreading, or how many deaths it has caused. While the drug has been in circulation for approximately six (6) years, there have been reports of it spreading to neighboring countries, including Liberia and Guinea, over the past two (2) years.

Kush, sometimes referred to as the "zombie drug," has been known to cause users to fall over or injure themselves due to falling asleep while walking. There have been reports of up to a dozen overdoses every week and thousands of hospitalizations. The drug is mixed with cannabis, fentanyl, tramadol, and formaldehyde. Open-source reports show that it is likely that at least a million people in the region have become addicted to the drug.

Analyst Comment

"Zombie drugs" are synthetic drugs that are chemically altered to imitate the effects of illegal narcotics. They often enter countries through illicit channels, including smuggling across borders. This presents challenges for border security and customs agencies tasked with intercepting illegal drug shipments. Furthermore, in regions where these "zombie drugs" are prevalent, their impact can destabilize communities, exacerbate social inequalities, and undermine the rule of law. This instability can have broader regional ramifications and may spill over into neighboring countries, leading to cross-border security challenges.

As stated earlier, the struggling economies in West Africa makes it difficult to collect data on mortalities and overdoses. With the way the drug has spread, it has the potential to reach into East Africa and other neighboring countries. To address the problem, West African governments need comprehensive strategies that encompass public health interventions, law enforcement efforts, border security measures, and international cooperation. This multidimensional approach aims to reduce the demand for the drugs, disrupt supply chains, and strengthen regulatory frameworks to mitigate the threats posed by these "zombie drugs" and others like them.

Sources

https://www.newsweek.com/drug-mix-kush-deadly-addictive-africa-1861393

https://www.npr.org/sections/goatsandsoda/2024/02/10/1229662975/kush-synthetic-drug-sierra-leone

https://www.albawaba.com/editors-choice/deadly-drug-made-bone-powder-spreading-west-africa-1555800

Hazards

Atmospheric River Storm Prompts Mudslide and Flooding Concerns for California – *Natural Hazards (Meteorological)*

Summary

Portions of Southern California were under a flood warning on 06 February 2024 as a recent storm, fueled by atmospheric rivers, moved through the region. Atmospheric rivers are narrow bands that transport water vapor and can cause extreme weather events. The storm moved from Northern California down to the Southern region, causing mudslides and power outages. On 05 February 2024, 11.87 inches of rain fell in a 24-hour period. Heavy rain, mudslides, and flooding events occurred while regions of Southern California remained under flood warnings. The heavy rainfall, along with thunderstorms and damaging winds, increased the chances of flash flooding, which occurred in portions of the San Joaquin and Sacramento valley, as well as segments of the Sierra Nevada.

Analyst Comment

Recent flooding has caused subsequent landslides and mudslides to occur and, since the ground is already saturated, it takes little rain for additional occurrences. The Los Angeles Fire Department dealt with 100 reports of flooding and more than 300 mudslide events. Individuals in canyon areas affected by recent fires were ordered to evacuate, as trees and brush that could hold back mud and debris flows had been burned in wildfires.

On Sunday, 04 February 2024, Governor Gavin Newsome declared a state of emergency in multiple counties. Flood advisories and flood watches were also issued throughout the region, with a flood forecast warning issued for San Diego County. Many of these counties house DoD installations, whose operations have been impacted by recent weather events and power outages in the area.

Another storm system was reported for the region over Easter weekend on 30 March 2024. The storm prompted flood watches and warnings for Ventura and Los Angeles Counties, excess rain, and mountain snow. Recent extreme weather, coupled with that in February, have the ability to impact the state's largest reservoir of Lake Shasta, the water levels of which have been increasing since the beginning of March after dropping eight (8) feet in late February. This drop is due to high water levels from the atmospheric storms in February. Future storms may also significantly increase Lake Shasta's water levels.

Sources

https://www.usatoday.com/story/weather/2024/02/06/southern-california-weather-floods-mudslides-atmospheric-river/72488247007/

https://data.usatoday.com/severe-weather-alerts-warnings-watches/

https://apnews.com/article/california-storms-atmospheric-river-d6920af2dbaead274a30229cdbba7d97

https://www.npr.org/2024/02/04/1228918306/a-second-wave-of-storms-is-slamming-parts-of-california-how-bad-will-it-get

https://timesofsandiego.com/life/2024/03/26/atmospheric-river-to-return-with-possibly-heavy-rain-snow-easter-weekend/

https://www.msn.com/en-us/weather/topstories/how-californias-largest-reservoir-could-change-after-next-storm/ar-BB1kj7Th

https://www.msn.com/en-us/weather/topstories/easter-weekend-storm-hits-southern-california-with-rain-and-mountain-snow/ar-BB1kNTak

Largest Wildfire in Texas History Burns Over a Million Acres – *Natural Hazards (Meteorological)*

Summary

On 26 February 2024, Texas reported the ignition of a wildfire that would become the largest wildfire in the state's history. The Smokehouse Creek Fire burned over a million acres while the Windy Deuce Fire burned more than 144,000 acres. Both fires have since been contained, but not after ravaging through the Texas panhandle.

The Smokehouse Creek fire started one (1) mile north of Stinnett and traveled east along the Canadian River into Hemphill and Roberts County. According to Texas Governor Greg Abbott, approximately 70% of Hemphill County was burned in the fire, leaving 47 families displaced. The recent fires destroyed hundreds of homes, ranches, and farms while also destroying livestock that is crucial to the U.S. beef industry.

After three (3) weeks of burning, the fires led to three (3) deaths. Open-source reports show that power lines were a significant cause in igniting the massive wildfires across the panhandle. Provider Xcel Energy acknowledged that their facilities took part in igniting the fires, but also stated that their facilities were properly maintained.

Analyst Comment

Wildfires can impact local, state, and national security in various ways. They strain resources and response capabilities, affecting the ability to address other emergencies. Additionally, wildfires can damage critical infrastructure, disrupt communication systems, and compromise the safety of citizens and DoD personnel alike. Environmental consequences such as air pollution, and destruction of ecosystems may also have tertiary effects on public health and agriculture.

Smoke from wildfires can pose ongoing health risks to DoD personnel and nearby communities, potentially impacting readiness and mission effectiveness. Wildfires are destructive, but their aftermath can also strain the resources and capabilities of the DoD, requiring coordinated efforts to mitigate their effects and ensure continued mission readiness.

Sources

https://www.nbcdfw.com/news/local/texas-news/largest-wildfire-in-texas-history-100-contained-800000-raised-to-help-farmers-ranchers/3492512/

https://www.fox7austin.com/news/texas-panhandle-fires-special-committee-to-investigate-cause-response

https://www.nbcdfw.com/news/local/texas-news/largest-wildfire-in-texas-history-100-contained-800000-raised-to-help-farmers-ranchers/3492512/

https://www.newschannel10.com/2024/03/17/largest-wildfire-texas-history-now-100-contained/

Potential Measles Exposure at Cincinnati/Northern Kentucky International Airport – *Natural Hazards (Biological)*

Summary

On 05 February 2024, the Ohio Department of Health (ODH) Director announced that some individuals may have been exposed to measles in the Cincinnati/Northern Kentucky International Airport on two (2) separate days in January 2024. Following reports of Ohio's first measles case of the year, contracted by a child from Montgomery County, Ohio, the ODH and the Centers for Disease Control and Prevention (CDC) are working to find those who may have been exposed. Potential exposure could have occurred on 27 January between 17:00 and 21:00 or 29 January between 20:30 and 23:30. The Virginia Department of Health also announced that in mid-January 2024, a person returning from international travel earlier in the month was infected with measles and transited through both Dulles International Airport and Reagan Washington National Airport. Health officials warned that the exposure was linked to Dulles International Airport's main terminal arrivals area on 03 January (from 16:00 to 20:00) and Terminal A in Reagan Washington National Airport on 04 January (from 14:30 to 18:30).

Analyst Comment

In 2023, Ohio recorded one (1) measles case. However, the state experienced an outbreak centered in central Ohio in 2022 and documented 90 cases that year. The national number of measles cases also decreased from 2022 to 2023, as the CDC recorded 56 cases compared to 121 in 2022. The number of measles cases in 2024 has already surpassed those in 2023 (as of 14 March 2024), and 17 U.S. jurisdictions have reported 58 measles cases. According to a CDC-issued Health Alert Network (HAN) Health Advisory on 18 March 2024, 54 of the 58 measles cases were linked to international travel.

Open-source reporting indicates that up to 90% of individuals who come into contact with a person with measles will become infected. According to the ODH, the measles virus can survive up to two (2) hours in the air where an infected individual coughs or sneezes. Between seven (7) to 14 days after contact with the virus, infected individuals can experience symptoms including high fever, cough, runny nose, and red, watery eyes. Two (2) to three (3) days after symptoms begin, tiny white spots (Koplik spots) can develop inside the mouth. The CDC and other infectious disease experts highlight that measles can be prevented with the MMR vaccine, which protects against measles, mumps, and rubella.

The CDC recommends that children receive two (2) doses of the MMR vaccine, as well as adults born after 1957 who are not vaccinated. According to the CDC, most of the 58 measles cases as of March 2024 are among children aged 12 months and older who were not inoculated. Therefore, all U.S. residents traveling to international destinations are advised to be current on their MMR vaccinations.

Between 01 January 2016 and 30 June 2019, five (5) confirmed measles cases were reported among all Military Health System (MHS) beneficiaries. Over this 3.5-year surveillance period, no cases of measles were reported among U.S. servicemembers. According to the Defense Health Agency, low case counts of measles, mumps, rubella, and varicella "confirm the effectiveness of the respective vaccine components among the large MHS beneficiary population."

Sources

https://odh.ohio.gov/media-center/odh-news-releases/odh-news-release-02-05-24

https://odh.ohio.gov/media-center/feature-stories/odh-news-release-02-03-24

https://www.cdc.gov/measles/symptoms/signs-symptoms.html

https://www.cdc.gov/measles/cases-outbreaks.html

https://www.nbcwashington.com/news/local/northern-virginia/virginia-officials-warn-of-potential-measles-exposure-at-dulles-reagan-airports/3516566

https://emergency.cdc.gov/han/2024/han00504.asp

https://health.mil/News/Articles/2019/10/01/Measles-Mumps-Rubella-and-Varicella

Biological Research Laboratory Leaks in the U.S.– *Natural Hazards (Biological)*

Summary

From 70 to 100 biological lab leaks occur in the U.S. per year, yet these incidents are rarely brought to the attention of the general public. Approximately 600 leaks were documented between 2015 and 2022, according to the Federal Select Agents Program. Research by the Government Accountability Office (GAO) indicates that current regulations are a patchwork of rules across different government agencies. This creates an environment of unclear oversight and reporting standards. In 2022, the GAO recommended that Congress create a government agency to oversee and regulate labs in a framework similar to the nuclear industry.

There are seven (7) biosafety level 4 (BSL4) labs and at least twice as many biosafety level 3 (BSL3) labs operating in the U.S. BSL3 labs are allowed to conduct research on microbes that can be either indigenous or exotic, and they can cause serious or potentially lethal diseases through respiratory transmission of, for example, Mycobacterium tuberculosis. BSL4 labs are allowed to work with microbes that are dangerous and exotic, posing a high risk of aerosol-transmitted infections. Infections caused by these microbes are frequently fatal and without treatment or vaccines. Examples include Ebola and Marburg. Entities operating BSL4 labs in the U.S. include the Centers for Disease Control and Prevention, National Institute of Allergy and Infectious Diseases, Department of Homeland Security, the U.S. Army Medical Research Institute for Infectious Diseases (USAMRIID), Department of General Services of the Commonwealth of Virginia, Southwest Foundation for Biomedical Research, as well as the University of Texas, Boston University, and Georgia State University.

Research suggests that lab leaks most often occur due to human error or equipment failure. Scientists have spilled the contents of test tubes and suffered bites and scratches from infected research animals. In some cases, researchers did not use or improperly used safety equipment. Poor practices such as emptying blood from infected monkeys down drain holes has been reported. Examples of these lab leaks include:

- *Vials of the smallpox virus were found in a cold room of an FDA laboratory instead of within proper security areas.*
- *Misuse of protective clothing at a biological lab at Tulane National Primate Research Center in Louisiana led to monkeys becoming sick and testing positive for Vietnamese Timebomb Fever.*
- *A student at Washington University School of Medicine accidentally pierced her protective suit and skin with a needle, giving here the Chikungunya virus.*
- *Unsterilized laboratory wastewater from the USAMRIID at Fort Detrick, MD, spewed out the top of a rusty 50,000-gallon outdoor holding tank in spite of having an automatic shutoff feature.*

Analyst Comment

The number of BSL4 labs in the U.S. is set to double in the coming years. Six (6) BSL4 labs are either under construction or in stages of planning, and the USAMRIID lab at Fort Deitrick is being expanded. Almost all of these labs are located in or near urban environments. The sharp increase in high security biolabs began in the early 2000's after the anthrax attacks in the U.S. and the multinational outbreak of severe acute respiratory syndrome (SARS). The increased number of labs coincides with the rising number of people working with dangerous pathogens, thus elevating the risk of an accidental release.

The U.S. government has a total of seven (7) agencies with some level of responsibility concerning lab safety. The framework of safety regulations has not kept up with the rapid growth in biological research. Recommendations to reform regulations were developed by the National Science Advisory Board for Biosecurity in March of 2023. Some examples include the development of an integrated approach to oversight, making federal department-level review of research proposals a requirement, and the creation of a process to expedite federal department level review in cases critical to national health concerns or national security, among others. many of the pathogens being researched within BSL3 and BSL4 labs are far more infectious and lethal than Covid-19. This create the potential for a future epidemic or pandemic. Congressional action to enhance regulations should be enacted to mitigate the chances of either.

Sources

https://www.dailymail.co.uk/health/article-13170559/data-lab-leak-incidents-us.html

https://www.theguardian.com/commentisfree/2023/may/30/lab-leaks-shrouded-secrecy

https://health.wusf.usf.edu/health-news-florida/2023-04-25/did-a-military-lab-spill-anthrax-into-public-waterways-book-reveals-details-of-a-us-leak

https://www.cdc.gov/training/quicklearns/biosafety/

https://osp.od.nih.gov/wp-content/uploads/2023/03/NSABB-Final-Report-Proposed-Biosecurity-Oversight-Framework-for-the-Future-of-Science.pdf

---

U.S. Air Force F-35A Suffers Millions in Damage After Ingesting a Flashlight at Luke Air Force Base, AZ – *Accidental Hazards (Human or Technologically Caused)*

Summary

A recent accident investigation report by the U.S. Air Force found that an F-35A operated by the 56th Fighter Wing at Luke Air Force Base, AZ, suffered almost $4 million in engine damage after ingesting a flashlight during a maintenance ground run on 15 March 2023. The F-35A's $14 million engine was damaged beyond local repair; however, no injuries were reported. According to the report, high winds, rain, thunderstorms, and lightning within five (5) nautical miles of the airfield initially delayed maintenance operations for one (1) hour

during the 15 March shift, which comprised three (3) maintainers. After the delay, the team was ordered to complete a Time Compliance Technical Directive (TCTD), which is issued to offer instructions to Air Force activities for "accomplishing one-time changes, modifications, or inspections of equipment, or installation of new equipment." The instructions of the TCTD, issued by the Joint Program Office, seek to mitigate the risk of an Augmenter Throttle Valve Pressure Tube (CP12) assembly rupture and resolve the discrepancy for the F-35 fleet.

To conduct the TCTD, the maintainers removed a panel and installed a metering plug into an engine fuel line. When the engine spun down following a fuel leak check, one (1) of the maintainers noticed "abnormal noises." Ultimately, one (1) maintainer left a flashlight used during a "Before Operations Servicing" (BOS) inspection inside the engine inlet. According to the investigation, failing to conduct a tool inventory check following the BOS inspection caused foreign object damage to the F-35 engine.

Analyst Comment

This incident highlights the potential impacts of foreign object debris (FOD), defined by the Naval Aviation Maintenance Program (NAMP) as "damage to aeronautical equipment, for example, aircraft, engines, missiles, drones, and SE caused by an object(s) external to the equipment." Examples of FOD include hardware, pavement fragments, rocks, trash, and other items. These objects are safety hazards and financial threats, especially during flight phases such as takeoff and landing rollout. According to a May 2023 FOD Detection System Cost-Benefit Analysis conducted by the Federal Aviation Administration (FAA), annual global costs of FOD range up to $22.7 billion (USD). Research examining engine foreign object damage (2020) found that at least 10 U.S. airports endure total annual FOD costs greater than $20 million. Furthermore, the FAA notes that secondary causes from FOD, such as delays and cancelations, also present significant consequences.

FOD can impact DOD operations through equipment damage, personnel injuries, and the implementation of various compliance measures. As highlighted in 354th Fighter Wing Instruction 21-135, general FOD prevention practices include flightline vehicle FOD prevention and individual responsibilities, such as performing inspections for FOD before finishing any maintenance task. Specific FOD prevention practices include air intake inspection, cockpit maintenance, installing protective covers, panel removal, and FOD walks.

Sources

https://www.airforcetimes.com/news/your-air-force/2024/01/19/misplaced-flashlight-in-f-35-engine-results-in-4-million-in-damage/

https://www.afjag.af.mil/Portals/77/AIB-Reports/2023/15%20MAR%202023,%20AETC,%20F-35A,%20Luke%20AFB,%20AIB%20Report.pdf

https://www.forbes.com/sites/erictegler/2024/01/19/the-air-force-lost-a-14-million-f-35-engine-because-of-a-flashlight/

https://www.navair.navy.mil/sites/g/files/jejdrs536/files/document/%5Bfilename%5D/15%20Feb%202022%204790.2D%20CH-1%20NAMP.pdf

https://www.defensenews.com/air/2024/03/12/f-35-upgrade-delays-prompt-us-air-force-to-scale-back-jet-purchases/

https://static.e-publishing.af.mil/production/1/354fw/publication/354fwi21-135/354fwi21-135.pdf

https://www.faa.gov/airports/airport_safety/fod

https://media.defense.gov/2019/Dec/19/2002227452/-1/1/1/FLIGHTFAX%2082_OCTOBER%202019_PAGES7-10.PDF
https://www.tc.faa.gov/its/worldpac/techrpt/tc22-47.pdf

https://www.lockheedmartin.com/content/dam/lockheed-martin/aero/documents/scm/tandc/FOD/fod.pdf

https://www.navy.mil/Press-Office/News-Stories/Article/3181225/nas-patuxent-river-promotes-safety-with-base-wide-fod-walk-down/

https://www.jber.jb.mil/News/Articles/Display/Article/3419402/3rd-wing-airmen-conduct-fod-walk/

Francis Scott Key Bridge Collapses – *Accidental Hazards (Human or Technologically Caused)*

Summary

The Francis Scott Key Bridge collapsed into the Patapsco River near Baltimore, MD, after it was struck by the container ship, Dali. The ship was departing the U.S., enroute to Sri Lanka. The U.S. Coast Guard (USCG) and local agencies responded immediately, followed by other federal assets, including a National Transportation Safety Board (NTSB) Go Team and the FBI. Recovery efforts are currently underway. The investigation into the cause of the incident is being led by the NTSB, which has a team of 24 experts who will evaluate the vessel's operations, safety history, records, and data recorder. The U.S. Army Corps of Engineers and U.S. Navy salvage teams are coordinating the cleanup efforts. The FBI and Baltimore Police quickly reported that there are no indications the collision was intentional or an act of terrorism.

The sequence of events leading up to the collision is becoming clearer now that the crew has been interviewed, the ship's data recorder has been recovered, and 911 operator tapes have been released, along with video of the incident. These sources indicate that the ship lost power, and backup generators began providing electrical power. The ship's crew issued a mayday call, which included a warning that a collision with the bridge was possible. This alerted police, who blocked traffic on both sides of the bridge. One (1) minute later, the Dali struck the column holding up the bridge before first responders could evacuate a construction crew working there. This sequence of event this occurred over the course of three (3) to four (4) minutes.

The construction crew of eight (8) workers was repairing potholes on the bridge at the time of the collision. They fell approximately 185 feet along with the structure. One (1) worker was hospitalized, one (1) was released from the scene with minor injuries, and six (6) lost their lives. Only three (3) of the deceased have been recovered at this time. Multiple vehicles on the bridge fell into the river as well. The Baltimore Fire Department reported four (4) vehicles and a cement truck were located underwater using infrared and side-scan sonar.

The Dali was built in 2015, has a gross tonnage of 95128 tons, and is 948 feet long. It is owned by Grace Ocean, a Singapore-based company. The ship is managed by Synergy Marine which is also based in Singapore. The Dali was chartered by international shipping company Maersk, who released a statement saying ships inbound to Baltimore will have to be rerouted to other east coast ports, creating shipping delays. The Dali was involved in another accident in 2016 when the ship struck a pier in Antwerp, Belgium. The stern of the ship was damaged in the incident. An investigation determined a mistake by the ship's master and pilot was the cause.

Analyst Comment

The impacts of the bridge collapse will be broad and severe. The Port of Baltimore is the ninth busiest port in the U.S. and the busiest port for vehicle imports. In 2023 the port unloaded at least 750,000 vehicles and processed $80 billion in foreign cargo. Baltimore is also the second busiest port in the U.S. for exporting coal, with most exports going to India. Ports exporting coal use specialized equipment, which makes rerouting the product difficult. The bridge was heavily used by Amazon and FedEx, who have distribution warehouses at the port.

This incident shows the vulnerability of bridges associated with large ports around the country. A similar collision can happen almost anywhere, raising questions about bridge construction techniques and methods of hardening existing bridges. Furthermore, there are concerns about what threat actors may learn from this incident. Some analysts have assessed that terrorists have not targeted bridges in the U.S. because of post-9/11 counter-terrorism measures, perceived structural soundness, and the overall expense and difficulty. This has historically made bridges less attractive than softer targets.

Following the collapse of the Francis Scot Key bridge, some analysts have postulated that a vessel could deliver enough explosives to collapse a similar structure. Although this incident was accidental, it shows that a large enough vessel without explosives can already create the same result. Additionally, a threat actor getting a ship into a U.S. port is not farfetched. In 2021, there were 73,974 port calls in U.S. ports. All of these visits require notification to the U.S. Coast Guard 96 hours before arrival. Based on multiple criteria, the U.S. Coast Guard decides which vessels will receive a Port State Control (PSC) Examination. PSC examinations were conducted on 8,663 of the 73,974 ships arriving in U.S. Ports in 2021, for a rate of less than 12%. While deeply tragic, this incident provides an opportunity to learn valuable lessons which can be applied to future critical infrastructure projects, as well as laws and policies regarding ship maintenance and operations.

Sources

https://news.usni.org/2024/03/26/coast-guard-heading-search-and-rescue-effort-after-container-ship-collapses-baltimore-bridge

https://www.news.uscg.mil/Press-Releases/Article/3718320/coast-guard-multiple-partners-agencies-responding-to-francis-scott-key-bridge-c/

https://www.dco.uscg.mil/Portals/9/DCO%20Documents/5p/CG-5PC/CG-CVC/CVC2/psc/AnnualReports/annualrpt21a.pdf

https://www.icct.nl/sites/default/files/2022-12/Deadly%20Detours%20final%20draft.pdf

https://www.cbsnews.com/news/francis-scott-key-bridge-collapse-timeline-911-call-dali-cargo-ship-mayday-maps-construction-worker-recovery/

On the Radar

- *The U.S. Army recorded at least a dozen aircraft mishaps in just the first six (6) months of this fiscal year. They have already matched the number of mishaps for fiscal year 2023. A Class A mishap in the U.S. Army is defined as a mishap that leads to loss of life or equipment exceeding $2.5 million. Currently, the rate of Class A mishaps is 3.22 and is more than double the rate of any of the last decade. To ensure stability, safety, and readiness, the U.S. Army has implemented additional aviation training throughout the entire force.*
- *In April 2024, about four (4) tons of diesel fuel spilled from Camp Mujuk near Pohang, South Korea, into a nearby stream. According to Marine Corps Forces Korea, the incident is under investigation. The Korean Federation for Environmental Movement, a non-governmental organization, called on Camp Mujuk's leaders to officially apologize after city workers collected 20 tons of water mixed with fuel from the stream. The mayor of Pohang requested that Camp Mujuk install an oil berm to prevent a similar spill and remove potentially contaminated soil.*
- *China has the largest navy in the world, comprised of three (3) aircraft carriers and an estimated three (3) helicopter carriers, 50 destroyers, 43 frigates, 72 corvettes, 78 submarines, 150 patrol vessels, and 36 mine warfare craft. The People's Liberation Army Navy (PLAN) is largely composed of modern multi-mission ships and submarines. A recently declassified intelligence slide from the Office of Naval Intelligence estimates that China has 232 times the shipbuilding capability of the United States, raising concerns around topics such as U.S. shipbuilding capacity, supply chain issues, U.S. Navy warship maintenance backlogs, and the overall U.S. Navy budget necessary to maintain parity with near-peer nation state competitors.*