**Risk Mitigation Consulting Inc.**

*Intelligence and Analysis Division*

# OPEN SOURCE UPDATE

## October 2021

INTENT

This open source periodical is designed to provide an overview of relevant, publicly available information on threat and hazard events and analysis of potential impacts to the interests of the United States, both at home and abroad. This product is not intended to be a comprehensive overview of all threat and hazard news and inclusion in this product does not constitute a confirmation of credibility nor precedence by RMC.

# Threats

## Dept. of Navy Civilian Attempts to Sell Nuclear Secrets – *Insider Threat*

**Summary:** A nuclear engineer employed by the Department of the Navy was arrested on 09 October 2021 for allegedly attempting to sell classified information to a foreign government. His wife, a high school teacher, was also arrested for participating in the plot. The two reside in Maryland but were arrested in Johnson County, West Virginia. The engineer left active Naval service in December 2020 after eight (8) years of service and was employed as a civilian. He had an active security clearance. Allegedly, on 01 April 2020, the engineer sent a package to an unnamed foreign government with a sample of classified information and an offer to sell more. Whomever received the package turned it in to the local FBI attaché. Federal agents corresponded with the engineer via encrypted e-mail, posing as representatives of the government. They brokered a deal to buy information for $10,000 in cryptocurrency. They later picked up a package in West Virginia, which proved the legitimacy of the engineer's claims. The undercover agents brokered two (2) more exchanges over the next year for larger amounts of cryptocurrency until the engineer and his wife were arrested. The information he provided included classified details about Virginia-class nuclear submarine reactors. The two (2) have been charged in a criminal complaint alleging violations of the Atomic Energy Act. Their initial appearance in court occurred on 12 October 2021.

**Analyst Comment:** The engineer's motivations may be strictly financial. However, any underlying causes have yet to be reported in open sources. His wife, who assisted in the plot, reportedly supported several progressive causes on social media and expressed antipathy towards former President Donald Trump. The former President was in office at the time of the engineer's initial contact. However, it is unclear if the engineer was motivated by any desire to undermine the United States. Oftentimes, personnel are targeted by agents of foreign governments who pose as friends or professional colleagues. They typically seek out vulnerable individuals who may be experiencing personal or financial difficulties. Once they have established a relationship with the target, they attempt to use them for access, sometimes offering financial compensation. In June 2021, a Department of Defense (DoD) linguist was sentenced to 23 years in prison for providing classified information to a romantic interest who had ties to Lebanese Hezbollah. DoD personnel occasionally attempt initial contact with foreign powers, usually for financial gain. They are rarely motivated by antipathy towards their own country. However, this also occurs. In 2006, a Navy fire control technician attempted to sell classified information to the Austrian government (and later, the Russian government) in exchange for asylum. Initially, he was pursuing a romantic interest who resided in Austria, but he also expressed anger over his tour of duty aboard a U.S. Navy submarine. He was subsequently discharged and sentenced to prison. The case of the Maryland nuclear engineer and his wife is still developing.

*Sources:* https://www.justice.gov/opa/pr/maryland-nuclear-engineer-and-spouse-arrested-espionage-related-charges

https://www.npr.org/2021/10/10/1044883780/nuclear-engineer-navy-and-wife-arrested-espionage-charges

https://www.washingtonpost.com/national-security/navy-nuclear-engineer-and-his-wife-charged-with-trying-to-share-submarine-secrets-with-a-foreign-country/2021/10/10/c461aff2-29d9-11ec-baf4-d7a4e075eb90_story.html

https://www.wusa9.com/article/news/crime/maryland-nuclear-engineer-wife-arrested-for-secret-military-data-foreign-power/65-79d3b181-d6c6-4688-8604-eaabf32393df

https://www.foxnews.com/us/wife-navy-nuclear-engineer-facebook-blm-feminism

https://www.justice.gov/opa/pr/defense-department-linguist-sentenced-23-years-prison-transmitting-highly-sensitive

https://www.dhra.mil/PERSEREC/Espionage-Cases/navy3/

## "Secretive U.S. Aircraft" Potentially Revealed on TikTok – *Insider Threat*

**Summary:** Operational security (OPSEC) concerns were raised after a brief video posted to the video sharing/social media app TikTok in September 2021 appeared to show a stealthy aircraft-like object being transported on a tractor trailer. Amateur open source intelligence practitioners on other social networks such as Twitter and Reddit have contended that the video was filmed at a Lockheed Martin-owned facility in California, based on analysis of the TikTok video.

In the wake of the video's circulation online, a number of defense reporters reached out to Lockheed Martin and United States Air Force personnel for comment. One reporter showed the video to General Mark Kelly (the Air Combat Command chief), who stated that he "had no idea" what the object in the video was. Another reporter asked General Charles Q. Brown (the Air Force's Chief of Staff) about the video, but General Brown stated that he was "not aware" of the particular recording and could not comment. The head of Lockheed Martin's secretive Skunk Works division (which oversees the firm's most secretive projects) declined to comment on the situation but added "we're good" when asked if the Lockheed site's security posture has been altered in the wake of the video's release.

**Analyst Comment:** Though the video's authenticity has not been confirmed by Lockheed Martin or U.S. government representatives, the Lockheed Martin-owned facility where the video was reportedly taken would likely be subject to various enhanced security/OPSEC policies, as it is reportedly home to testing activities related to stealth technologies.

Insider threats can be malicious or non-malicious in nature. Malicious insider threats include deliberate theft of sensitive information for espionage purposes, as well as acts such as active shooter events and terrorism. Conversely, non-malicious insider threats generally emanate from carelessness, failure to observe policies/procedures, and insufficient training.

This incident could potentially be indicative of a malicious insider threat if the video (assuming it is authentic) was deliberately released with malicious intent. Alternatively, the video could have been filmed by a careless bystander who may not be fully aware of security policies in effect on the site. This would constitute a non-malicious insider threat.

Similar non-malicious insider threats could occur onboard DoD installations from transient visitors such as taxi drivers and truck drivers, if they misuse personal electronic devices for purposes such as unauthorized photography/videography. Though not intending to harm U.S. national security, these individuals could potentially provide U.S. adversaries with pieces of information that could potentially be exploited.

*Sources:* https://warisboring.com/secret-military-aircraft-possibly-exposed-on-tiktok/

https://www.thedrive.com/the-war-zone/42568/skunk-works-boss-says-he-cant-comment-on-video-of-mysterious-stealth-shape-at-radar-test-range

https://www.thedrive.com/the-war-zone/42480/mysterious-stealthy-shape-that-resembles-future-fighter-concepts-spotted-at-radar-test-range

https://www.thedrive.com/the-war-zone/15746/lockheeds-helendale-radar-signature-test-range-looks-right-out-of-science-fiction

https://theaviationist.com/2021/09/22/mysterious-shape-helendale/

## China Tests Hypersonic Glider with Space Capability – *Foreign Nation-State Military*

**Summary:** U.S. intelligence services recently learned that China may have test-launched a rocket bearing a hypersonic glide vehicle in July or August from Jiuquan, which circled the globe before possibly landing at Badajilin or Youqi Airport. Conflicting reports in open source media suggested that the vehicle missed its target by two (2) dozen miles, while others suggest that it landed at one of the airports as intended. Initial reports have also disagreed over whether the flight was suborbital or, in fact, orbital. The launch raises concerns about the country's ability to put a nuclear weapon into space using the same technology, which could reach a target on the other side of the globe. The U.S., Russia, and China are all developing hypersonic weapons, including the aforementioned glide vehicles that are launched into space on a rocket. They orbit the earth under their own momentum, flying at five (5) times the speed of sound, which is slower than a ballistic missile but six (6) times faster than a Tomahawk missile. They also do not follow the fixed trajectory of a ballistic missile, and they are maneuverable, which makes them harder to track. China's Foreign Ministry denied that the country had tested a nuclear-capable hypersonic missile, per se. It claimed that the launch was a routine test of a space vehicle. However, the launch itself is less of a cause for concern than the potential to use the same technology for offensive purposes. Experts speaking in open sources stated that the successful tests by China mean the country is capable of orbital bombardment. A hypersonic glide vehicle armed with a nuclear warhead could evade U.S. missile defense systems that are designed to destroy incoming ballistic missiles.

**Analyst Comment:** China's continued technological march forward is cause for alarm. The launch in question follows the recent discovery of new missile silos in China's desert. The U.S. is left attempting to escalate its missile defense capabilities to respond to this emerging generation of hypersonic weapons. The conflicting details reported in open source media complicate the situation. A miss of two (2) dozen miles by a space vehicle is of less concern than a hypersonic glider with a nuclear payload striking within as many miles of its target. Some calmer voices in open source media still point to mutually assured destruction as a deterrent to China's nuclear capabilities. In other words, while they may have the ability to launch a nuclear weapon into space against a target on the other side of the planet, they are unlikely to do so, given the inevitable response. However, while the prospect of full-scale nuclear war is unlikely in the near future, the escalation of capabilities by China gives it strategic leverage on the global stage. This influences its economic posture towards the U.S. as well as more overt moves towards Taiwan and other regional competitors.

*Sources:* https://www.ft.com/content/ba0a3cde-719b-4040-93cb-a486e1f843fb

https://sattrackcam.blogspot.com/2021/10/a-chinese-fobs-surprise-and-other-stuff.html

https://sattrackcam.blogspot.com/2021/10/the-chinese-space-plane-test-of-16-july.html

https://allthingsnuclear.org/ctracy/how-do-hypersonic-weapons-work/

https://www.reuters.com/world/china/china-joins-heated-race-new-missiles-vies-with-us-russia-2021-10-18/

https://www.wsj.com/articles/chinas-hypersonic-wake-up-call-11634596933

## Confucius Institute in Indiana Draws Scrutiny from State Attorney General – *Foreign Intelligence Entities*

**Summary:** Indiana Attorney General Todd Rokita recently announced his office is launching a civil investigation into Valparaiso University and Chinese cultural institution the Confucius Institute over fears the relationship between the two is promoting communist propaganda in Indiana.

The attorney general's office declined to tell a local media outlet what specific evidence it has supporting the insinuation that Beijing is attempting to spread propaganda through the Valparaiso University-Confucius Institute relationship, which partially relies on funds from the Chinese government. "We are not able to comment on the specifics of an ongoing investigation," a spokesperson said.

A Valparaiso University statement denied any wrongdoing or noncompliance, stating that the University (a Lutheran-affiliated institution) "does not and would not support any kind of endeavor

that furthers or promotes communist ideology as doing so would conflict with its Christian mission and purpose and its strong support of the First Amendment of the U.S. Constitution that protects the freedom of speech and religion."

**Analyst Comment:** Though there is currently no publicly available evidence to support specific acts of wrongdoing related to the Confucius Institute at Valparaiso University, Confucius Institutes have faced significant scrutiny in recent years. In 2020, the Trump administration designated the parent organization of Confucius Institutes as a "foreign mission" of the People's Republic of China (PRC), requiring regular operational disclosures to the Department of State.

A 2021 Congressional Research Service (CRS) report states that "some reports provide examples of Confucius Institute Board members or PRC officials directly or indirectly pressuring faculty, administrators, or invited guests at U.S. universities that host Confucius Institutes to avoid making public statements or holding events on topics that the Chinese government considers politically sensitive." Conversely, the CRS report notes that "other reports suggest that there have been few instances of Confucius Institutes overtly attempting to interfere in academic and extra-curricular activities and speech at U.S. host universities."

Though Confucius Institutes at U.S. universities primarily serve as a platform for cultural exchange, the potential remains for Confucius Institutes to continue amplifying PRC messaging within the U.S., as well as stifling messaging that runs counter to the PRC's. Moreover, some U.S. lawmakers have asserted that Confucius Institutes could also potentially serve as a platform for Chinese espionage efforts.

*Sources:* https://www.msn.com/en-us/news/world/valparaiso-university-responds-to-ags-concern-china-is-infiltrating-indiana-schools/ar-AANcrwS

https://crsreports.congress.gov/product/pdf/IF/IF11180

https://www.npr.org/2019/07/17/741239298/as-scrutiny-of-china-grows-some-u-s-schools-drop-a-language-program

## Homicide Rates Experience Large Increase in 2020 – *Violent Crime*

**Summary:** Per FBI and CDC data, homicides in the U.S. experienced a nearly 30% increase in 2020. This is the largest jump seen since record keeping began in the 1960s. Homicides and non-negligent manslaughters climbed an estimated 29.4% to 21,570, an increase of 4,901 over 2019. It is the highest estimated total since the early 1990s, when homicides were above 23,000 a year. Additionally, violent crimes in 2020 went up by a more moderate 5.6% over the previous year while property crimes continued a nearly two-decade decline, falling 7.8%. Robbery and rape dropped 9.3% and 12% respectively. Property crimes continued their long trend of decline and dropped 8% from 2019.

**Analyst Comment:** A myriad of factors likely combined to result in this dramatic uptick in homicides. The unique environment created by the ongoing pandemic and lockdowns of 2020 as

well as the high intensity political and social environment contributed to this unique and selective increase. Notably, the percentage of murders increased in cities with a population between 10,000 and 25,000 than in cities of 250,000 to 1 million. This shows incidents to be more geographically scattered. For example, in the 1990s, New York and Los Angeles accounted for 13.5% of all murders nationally but last year accounted for 4%. Firearms were the primary driver of the violence, as 77% of murders were committed with a gun. This statistic has been slowly increasing in recent years.

*Sources:* https://www.latimes.com/world-nation/story/2021-09-27/fbi-2020-homicides-up-nearly-30-largest-1-year-jump-ever

https://www.npr.org/2021/09/27/1040904770/fbi-data-murder-increase-2020

https://www.cnn.com/2021/09/27/politics/uniform-crime-report-2020/index.html

https://www.cbs58.com/news/us-records-highest-increase-in-nations-homicide-rate-in-modern-history-cdc-says

## 106 Italian Mafia Members Arrested for Cybercrime, Other Offenses

***– Gang Activity***

**Summary:** Per a 20 September 2021 Europol press release, the Spanish National Police (Policía Nacional), supported by the Italian National Police (Polizia di Stato), Europol and Eurojust, dismantled an organized crime group linked to the Italian Mafia involved in online fraud, money laundering, drug trafficking and property crime.

Per cybersecurity firm Recorded Future, the group executed SIM swapping attacks, phishing, and "vishing" (voice phishing) in order to breach company networks and steal funds or trick employees into sending payments to the wrong accounts in a classic scheme called "CEO fraud" or "BEC scam." Using these tactics, the group stole and later laundered more than €10 million (~$11.7 million) in stolen funds, using a network of money mules and shell companies. Most of the victimized companies were based in Italy, but the group also defrauded and scammed companies from Ireland, Spain, Germany, Lithuania, and the UK.

**Analyst Comment:** The recent arrests highlight an ongoing trend among organized crime groups toward diversified money-making efforts, to include operations within cyberspace. Traditional methods of organized crime (such as drug trafficking, human trafficking, and extortion) remain prevalent, though malicious cyber activity remains an ever-growing threat. Still, a significant amount of cybercrime is perpetrated by loose groups of hackers who do not share the organizational structures or coordination of traditional organized crime groups.

The Italian Mafia members' hacking did not involve sophisticated tactics including technical exploitation of networks. Rather, it relied primarily on basic social engineering, in which phishing emails and other fraudulent communications allow malicious actors to compromise login

information and establish quasi-legitimate access to their desired networks. Individuals should remain vigilant for phishing and "vishing" activity, in which malicious actors may use phone calls or suspicious emails to obtain network credentials or other sensitive information (to include personally identifiable information).

*Sources:* https://www.europol.europa.eu/newsroom/news/106-arrested-in-sting-against-online-fraudsters

https://therecord.media/106-italian-mafia-members-arrested-for-sim-swapping-bec-scams-phishing/

https://msutoday.msu.edu/news/2020/organized-cybercrime-not-your-average-mafia

## Austin Man Arrested Following Arson Attempt on Democratic Offices – *Civil Disturbance*

**Summary:** An Austin man has been charged for arson and vandalism at the Travis County Democratic Party Coordinated Campaign building on 29 September 2021. Surveillance video showed the accused wearing an American flag bandanna over his face while throwing a rock and carrying a Molotov cocktail. The Molotov cocktail was thrown through a window, but it did not detonate as intended. However, it started a small fire in the office. Employees at a business next door put out the flames with an extinguisher. Security camera footage from two (2) hours later also implicated the same man in vandalism at the county's Ned Granger Administrative Building. That building was previously vandalized in January 2021. The Travis County Democratic Party's offices were also vandalized with political graffiti in November 2020. The man accused of the 29 September attacks there also reportedly left a note with threats of further political violence. A citizen later contacted investigators with incriminating text messages, purportedly from the accused. Investigators used the man's social media page to match the writing style. Authorities have charged him with arson and possessing a prohibited weapon. He was booked into the Travis County jail on bail of $40,000. Open sources also indicate he is being detained for a possible federal felony charge.

**Analyst Comment:** Like many major American cities, Austin has experienced a sharp increase in protests and demonstrations since last year, some of which have become violent. Racial justice protests in May 2020 descended into rioting and looting. In July 2020, a U.S. Army sergeant admitted to shooting an armed protestor from his vehicle. He was indicted, but he maintains that he acted in self-defense. The acts of vandalism against the Travis County Democratic Party's offices and the Ned Granger building suggest a continued rise in hostility concurrent with national trends. The vandalism on the Democratic Party's offices in November 2020 included minor structural damage and graffiti in support of communism. The most recent attacks were very likely right-wing in nature. Recent protests in Austin have also been attended by armed right-wing militia members. Prior to that, in January 2021, the Texas Department of Public Safety closed the state Capitol after receiving threat intelligence related to the Presidential Inauguration. The use of an incendiary device against a political target by a right-wing actor is a clear escalation. Each

perceived slight or incident perpetrated by either side of the conflict has the potential to elevate hostilities and elicit a response. This will continue a mounting cycle of political violence that has no immediate end in sight.

*Sources:* https://apnews.com/article/fires-austin-texas-0d88e008e385feb7001be133f19c11c0

https://www.statesman.com/story/news/2021/09/29/molotov-cocktail-travis-county-democrat-office-austin/5914256001/

https://www.kvue.com/article/news/crime/travis-county-buildings-vandalized/269-8ad8eea1-f7ec-41ef-a871-ebcd4490da3e

https://www.texastribune.org/2021/07/01/garrett-foster-indicted-murder-daniel-perry-austin-protester/

https://www.austinchronicle.com/news/2021-09-24/pressure-grows-for-austin-to-settle-with-protesters-injured-by-apd/

https://www.texastribune.org/2020/08/02/austin-protest-garrett-foster/

https://www.kxan.com/news/local/austin/some-businesses-looted-fires-set-as-downtown-austin-protests-continue-into-the-night/

https://www.statesman.com/story/news/politics/2021/01/15/texas-readies-fbi-warns-state-capitols-protest-threats/4174667001/

# Hazards

## DoD Still Challenged by Unvaccinated Personnel - *Biological*

**Summary:** The first deadlines for Department of Defense (DoD) personnel to be fully vaccinated against COVID-19 are approaching. Each service is handling the logistics of administering the COMIRNATY vaccine from Pfizer/BioNTech to active, reserve, and National Guard personnel. Each service has set its own deadlines. The deadline for the Air Force is 02 November 2021 for active duty Airmen and Space Force Guardians and 02 December 2021 for reservists and the Air National Guard. The deadline for the Navy is 28 November 2021 for active duty Sailors, while the date for reservists is 28 December 2021. All active duty Marines must be fully vaccinated by 14 November 2021, and all reserve Marines must be fully vaccinated by 14 December 2021. The Army deadline for all active duty service members is 15 December 2021, while reservists and the National Guard have until 30 June 2022. The extended deadlines are purportedly to accommodate reservists and National Guard personnel who may live at a significant distance from a military medical facility. In September 2021, more military personnel died from COVID-19 than in all of 2020, none of whom were fully vaccinated. However, as of early October 2021, more than 92% of active-duty troops have received at least one dose. The vaccine mandate has generated controversy in the ranks. In late September 2021, two (2) servicemembers filed a class action lawsuit against Defense Secretary Lloyd Austin to halt the mandate. They requested an exemption for those who were previously infected with the virus due to the presence of antibodies. As of now, personnel who refuse the vaccine without a religious or medical exemption will face disciplinary action up to and including discharge, depending on the service.

**Analyst Comment:** Servicemembers are accustomed to receiving multiple vaccines throughout their military career. However, a small percentage of servicemembers do not want the COMIRNATY vaccine for COVID-19. Their reasons range from concerns over the expedited development of the vaccine, to religious concerns, to misinformation perpetuated on social media. Regardless of their justification, it is safe to assume that many will acquiesce by the deadlines set by their respective services. Still others will accept disciplinary action, up to and including a discharge. Each service has its own procedures for reprimanding those who refuse the vaccine. The Navy has suggested that simple refusal of the vaccine without an exemption could lead to a general discharge under honorable conditions, depending on the overall character of the individual's service. Servicemembers who refuse the vaccine present the DoD with two (2) challenges. First, a wave of disciplinary actions and separations could impact operational readiness. Second, unvaccinated personnel with an exemption, however justifiable, may still contract COVID-19 and spread it within their unit and beyond. A unit that contracts COVID-19 would be forced to seek medical treatment and quarantine. Individuals with exemptions may also be difficult or even unable to deploy overseas. Some personnel are prepared to separate from military service over this issue. This will undoubtedly impact operational readiness, but the degree to which depends on the DoD's ability to persuade servicemembers to accept the vaccine in the coming weeks and months.

As of 20 October, the DoD has fully vaccinated 1,431,012 service members, to include the members of the reserve force. The U.S. military isn't the only leading world power attempting to

ensure its members are vaccinated. Comparatively, Open Source reporting reveals that as of earlier this year over 400,000 Russian service members have been fully vaccinated while more than 530,000 have received at least their first dose. Additionally, the Global Times, a Chinese state media publication, reveals China intends to inoculate 100% of the People's Liberation Army against COVID-19, and may very well be close to achieving that goal. Despite the veracity of these claims, it is likely that the first military that can achieve its vaccination goals will maintain the operational edge, at least in the short term.

*Sources:* https://www.health.mil/News/Articles/2021/09/20/Deadlines-set-for-all-service-members-vaccinations-against-COVID

https://www.marines.mil/News/Messages/Messages-Display/Article/2803707/supplemental-guidance-to-mandatory-covid-19-vaccination-of-marine-corps-active/

https://www.stripes.com/covid/2021-10-10/us-military-covid-vaccine-mandate-unvaccinated-3191964.html

https://www.military.com/daily-news/2021/10/07/92-of-active-duty-troops-have-been-vaccinated-mandatory-deadline-nears.html

https://www.stripes.com/covid/2021-09-29/coronavirus-vaccine-military-mandate-lawsuit-service-members-3070322.html

https://www.navytimes.com/news/your-navy/2021/10/14/navy-unveils-discharge-plans-for-sailors-who-refuse-covid-19-vaccine/

https://www.newsweek.com/60000-air-force-personnel-face-punishment-failing-comply-vaccine-mandate-1637522

https://www.nytimes.com/2021/02/27/us/politics/coronavirus-vaccine-refusal-military.html

https://www.military.com/daily-news/2021/09/14/soldiers-have-3-months-get-covid-vaccine-or-face-discharge-few-waiver-options.html

## Oil Spill in Orange County, CA – *Accidental Events*

**Summary:** Beginning on 01 October, Orange County, CA shores began smelling of petroleum. An oil sheen could be seen on the water, and it was shortly thereafter confirmed that an oil spill occurred. Initial estimates put leak between 25,000-132,000 gallons. The leak occurred about 5 miles (8 kilometers) offshore at a depth of about 98 feet (30 meters) and came from a pipeline owned by Amplify Energy. Amplify's CEO reported the company did not discover the leak until it saw oil in the water at 8:09 a.m. on 02 October, then notified California Emergency Services within an hour. After two weeks the estimate was revised to be close to the lower estimate of 25,000 gallons, as 588 barrels were spilled.

**Analyst Comment:** The environmental impact of oil spills along coast lines effects both the local ecosystem, health of residents of the area, and businesses that rely on coastal business or transit. The impacts are dependent on the amount of oil spilled. So far, environmental impacts of this spill have been minimal and cleanup efforts are underway. Fishing is still barred in the area, and more than 4 dozen animals have been found dead in the area. Additionally, the U.S. Coast Guard has removed about 1,281 gallons of an "oily water mixture." Thousands of gallons of oily water mixture have been recovered from the water and beaches by the Coast Guard and other response teams.
The cause of the spill is still being determined, but recent reports have revealed that the subsea pipeline the spill originated from may have been damaged. Several months prior to the spill, a 1,200-foot cargo ship dropped its anchor in rough seas. As the anchor dragged, it caught the oil pipeline and pulled it across the seafloor. This impact knocked the concrete protective casing off of the pipe and dragged it about 105 feet, causing significant bending but no immediate break. This bend in the pipe was found by U.S. Coast Guard divers shortly after the spill occurred. Investigators have suggested that following this initial event, other ships' anchors may have also struck the displaced pipe.

*Sources:* https://www.cbsnews.com/news/california-oil-spill-much-smaller-than-originally-feared/

https://abcnews.go.com/US/wireStory/explainer-happening-california-oil-spill-80496721

https://www.usatoday.com/story/news/nation/2021/10/17/california-oil-spill-cargo-ship-dragged-pipeline/8502683002/

https://www.reuters.com/world/us/us-coast-guard-boards-ship-connection-with-california-oil-spill-2021-10-17/

https://www.msn.com/en-us/news/world/coast-guard-investigates-vessel-following-california-oil-spill/ar-AAPDoPT

## U.S. Navy Submarine Collides with "Underwater Object" in the South China Sea – *Accidental Events*

**Summary:** On 02 October 2021, the Seawolf-class nuclear attack submarine USS Connecticut (SSN-22) suffered an underwater collision while operating in international waters in the South China Sea. U.S. officials stated that about 11 sailors were hurt in the incident with moderate to minor injuries, none of which were life-threatening. Officials also stated that the submarine's nuclear propulsion systems were not affected, and the submarine was in transit to Guam (sailing on the surface) pending further assessment and investigation.

**Analyst Comment:** RMC's Intelligence and Analysis Division tracks events such as this one as "maritime mishaps," which are any marine casualty or accident (as defined by the U.S. Code of Federal Regulations) that affects DoD operations.

The U.S. Navy and its contractors maintain a safety program known as SUBSAFE, which involves "rigorous checks in design, manufacture, and maintenance" in order to ensure that submarines would be able to rapidly surface in the event of an emergency.

The last known similar incident occurred in 2005, when the Los Angeles-class nuclear submarine USS San Francisco (SSN-711) ran full speed into an underwater mountain near Guam more than 500 feet below the ocean's surface. One Sailor was killed in the incident as a result of a head injury, and 98 other crewmembers were injured. An investigation found that voyage planning and navigation errors led to the collision.

Other incidents involving surface vessels have occurred in the region in recent years, to include a pair of incidents in 2017 in which the USS Fitzgerald and the USS John McCain (both Arleigh Burke-class destroyers) were involved in collisions with commercial vessels in the Indo-Pacific Command region just a few months apart. In the USS Fitzgerald incident, 7 Sailors were killed, and 3 others were injured. In the USS John McCain incident, 10 Sailors were killed, and 5 others were injured. Each incident also resulted in millions of dollars in damages.

*Sources:* https://news.usni.org/2021/10/07/breaking-attack-submarine-uss-connecticut-suffers-underwater-in-pacific

https://news.usni.org/2013/04/04/after-thresher-how-the-navy-made-subs-safer

https://www.cbsnews.com/news/whos-to-blame-for-sub-accident/

https://www.marinelink.com/news/investigation-francisco316552

https://www.bbc.com/news/world-asia-40310563

https://www.military.com/daily-news/2017/11/01/confusion-steering-put-uss-mccain-deadly-collision-course.html

# In the Spotlight

## Cascading Impacts of the Facebook Outage – *Cyber, Accidental Disruption*

On 04 October, the Facebook network data centers experienced a massive outage for over six hours. A cascade of problems resulted, impacting millions across the globe. Per Facebook, this was caused by a glitch during routine maintenance. The Vice President of Facebook reported a command was issued by engineers that was supposed to assess the availability of the backbone network that connects all of Facebook's disparate computing facilities. Instead, it unintentionally disconnected Facebook data centers from the rest of the world. Though the internal audit system should have audited commands to prevent mistakes, the tool itself contained a bug a failed to stop the command. When the data centers were disconnected, Facebook's DNS (Domain Name System) servers couldn't connect to the primary data centers. Then, the servers stopped advertising the border gateway protocol routing information needed by any device trying to connect to the server. This made the DNS servers operational but unreachable.

The resulting issues exacerbated the situation by hindering repairs. Facebook employees found the outage blocked internal tools, security systems stopped functioning, and the internal communication platform was down. This included tools that engineers would normally use to investigate and repair such outages. Engineers were sent onsite to the data centers to carryout repairs. However, once onsite, the engineers struggled to get inside the building containing the data centers due to physical and system security systems. Facebook employees found they were unable to enter buildings and conference room as the digital badges carried by employees were unable to be used. The integration of technology into physical security creates new vulnerabilities and points of failure that may only become apparent when breakdowns such as these occurs.

Billions of users found Facebook and its family of apps, including Instagram, Oculus, Messenger, and WhatsApp, had all crashed, preventing both casual use of social media, and important communications by those who rely on one or more of the apps. As of July 2021, roughly 3.51 billion people use one of these apps every month. For example, many Latin-American countries rely on using WhatsApp for primary communication, rather than texting or calling through a mobile carrier. Other countries such as India rely on Facebook as their primary source of internet use. Additionally, Facebook accounts serve as login requirements for many services. With the network down, users were unable to login to devices such as smart TVs, thermostats and other internet-connected devices that utilized a Facebook account. Any websites that relied on Facebook profiles for accounts, such as online shopping services were also impacted. Businesses that carried out sales via Facebook pages were unable to make sales or market during the outage. Services were gradually restored, but the cascading issues, both technological and economic, highlighted the vulnerabilities created by massive, interdependent services. It is important to note that this was not a malicious attack, and no user data was compromised. Rather, human error combined with technological failures created one of the largest outages in recent years.

*Sources:* https://news.cgtn.com/news/2021-10-06/Facebook-says-system-crash-caused-by-error-amid-ex-employee-hearing-148bNCNPO7e/index.html

https://www.nytimes.com/2021/10/04/technology/facebook-down.html

https://www.nytimes.com/2021/07/28/business/facebook-q2-earnings.html

https://www.engadget.com/facebook-outage-explainer-193155776.html

https://engineering.fb.com/2021/10/05/networking-traffic/outage-details/

https://www.cbsnews.com/news/facebook-instagram-whatsapp-outage/

https://www.theguardian.com/technology/2021/oct/05/the-global-outage-just-adds-to-facebooks-many-recent-woes

https://www.thenationalnews.com/world/2021/10/05/what-caused-facebook-and-whatsapp-to-crash/

# On the Radar

- ## Tensions in Taiwan
  - Tensions in Taiwan remain high following a large number of recent intrusions into Taiwan's Air Defense Identification Zone by Chinese military aircraft. Although China has historically sought a full 'reunification' of China (including Taiwan), President Xi Jinping recently stated that the largest obstacle was the "Taiwan independence force," adding that "those who forget their heritage, betray their motherland and seek to split the country will come to no good." Several military experts have assessed that China already has the military capabilities to conduct a successful invasion of Taiwan but may be hesitant to do so for a variety of reason to include potential casualties as well as a U.S. military response.
- ## New COVID-19 Variants May Undermine Progress
  - Scientists and public health officials are warning that future iterations of the COVID-19 virus may be resistant to vaccines and even more communicable than the Delta variant. While infections are down across the U.S., the virus still has the potential to mutate and spread, undoing much of the progress made over the past year.
- ## Santa Ana Winds
  - Though the Santa Ana winds of California can occur at any time, they are most frequent in the fall. When combined with existing wildfires, these intense, hot winds can lead to the intensification and increasingly rapid spread of wildfires in the region. Warnings have recently been issued regarding Santa Ana winds in Southern California as critical fire weather combines with these winds.