Open Source Update: July 2023

Intelligence & Analysis Division
Open Source Update

July 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

Military Personnel with Early Discharges Prominent Among Extremists – *Insider Threat*

Summary

The National Consortium for the Study of Terrorism and Responses to Terrorism (START) has identified 32 individuals charged with extremist plots and crimes over the past three (3) decades who were discharged from the military within weeks or months of enlistment. The total number of incidents for the same time period is approximately 3,000. The total number of individuals with military service numbered approximately 450. The crimes included mail bombings, bank robberies, mass shootings, and/or attempts to commit those crimes. Almost half committed or plotted mass casualty attacks, in which there are four (4) or more victims injured or killed. The reasons are multifaceted. Some may harbor grievances towards the military. They may also be recruited by extremist groups in search of disgruntled former personnel. Some may have harbored racial animus before joining. The 32 crimes date back to 1994. Fifteen (15) were committed by individuals affiliated with white supremacist groups. A military background was the most commonly shared characteristic among the perpetrators who executed or plotted mass casualty attacks, more so than criminal histories or mental health issues. Those who were discharged early were even more likely to be involved. Of the approximately 3,000 considered, those discharged during basic training were more than twice as likely to plan or execute mass casualty events. Of the 32 in question, approximately half were separated due psychological issues, while others were physically unfit or were removed for desertion or bad conduct. Three (3) of the 32 executed successful mass casualty attacks. Two (2) other attacks were deadly but killed fewer than four (4). The Department of Defense (DoD) recently added extremism education to its out-processing program for active-duty personnel, but this training is typically handled by individual branches of the Armed Forces for personnel being separated under normal circumstances.

The rate of extremism-driven crimes by enlistees with an early discharge has increased in recent years. Approximately one-third (1/3) of the 32 cases in question have occurred since 2020. Half of that group was affiliated with white supremacist, involuntary celibate ("incel"), or neo-Nazi groups. According to the Government Accountability Office, domestic terrorism increased by 357% between 2013 and 2021, and racially- or ethnically-motivated extremists committed the most violent crimes during that time. That trend is reflected in the aforementioned 32 cases. Most were affiliated with at least one (1) extremist organization, with about 45% belonging to white supremacy groups and 22% supporting al-Qaeda, the Taliban, or the Islamic State. Of the 32 cases, two (2) were convicted for their participation in the events of 06 January 2021 at the U.S. Capitol.

Analyst Comment

While the DoD considers its options, disgruntled former military personnel, particularly those discharged early, continue to pose a threat to installations, assets, and personnel. They may resent the military for rejecting them and may strike DoD targets in retaliation. They may have knowledge of access policies and procedures or possess old credentials that would allow them to enter an installation. They may also strike civilians, dependents, and other

targets in communities surrounding military bases. Such an attack could impact an installation and its personnel. The DoD is still grappling with the problem of how to educate enlistees leaving the service due to misconduct or under other-than-honorable or dishonorable circumstances. They are less likely to be receptive to counterextremism programs and more likely to harbor animus against the military, the government, and society at large.

Sources

https://www.navytimes.com/flashpoints/extremism-disinformation/2023/06/21/failed-military-recruits-prove-deadly-outliers/

https://www.start.umd.edu/profiles-individual-radicalization-united-states-pirus-keshif

---

National Parks Service Removes Cameras Overlooking San Diego Bay – *Foreign Intelligence Entities (FIE)*

Summary

In April 2023, the National Parks Service (NPS) confirmed that it had removed two (2) cameras at the Cabrillo National Monument following force protection concerns from the Naval Criminal Investigative Service (NCIS). According to NCIS, the private webcams and its YouTube channel offered access to 24-hour monitoring of vessels and assets located onboard Naval Air Station North Island, California. Specifically, an NCIS spokesperson noted that the webcams offered visuals of aircraft hangers and flight lines, Naval Base Point Loma submarine assets, and the movement of military personnel onboard Naval Base Coronado.

Open-source information indicates that approximately six (6) million people viewed footage from the cameras last year. In November 2022, footage of the near-miss between the SS Harpers Ferry (LSD-49) and guided-missile destroyer USS Momsen (DDG-92) was filmed on one (1) of the two (2) webcams from the Cabrillo National Monument. According to a report released a few days after the cameras were removed, investigators used the webcam footage to analyze the near-miss event. While the webcam founder noted that the cameras had been operating for more than 10 years, an NCIS spokesperson indicated that the request to have NPS remove the cameras "was not related to the Harpers Ferry/Momsen incident." Open-source reporting notes that the webcam founder and his group have other cameras in San Diego Bay and were scouting sites for cameras to replace the two (2) removed at the Cabrillo National Monument.

Analyst Comment

Cameras or other technology used to view DoD assets can impact force protection. According to the DCSA, individuals, such as foreign intelligence operatives, can engage in the surveillance of equipment, facilities, sites, and/or personnel, allowing them to potentially identify vulnerabilities. Over the past few years, concerns have been raised about surveillance cameras produced by Chinese manufacturers watching U.S. military bases. For example, in 2018, Fort Leonard Wood, Missouri, replaced five (5) cameras produced by Hangzhou Hikvision Digital Technology, which is 42% owned by the Chinese government. Open-source

reporting indicates that the technology has been used at other DoD installations and facilities, including Peterson Air Force Base in Colorado and a U.S. Navy research base in Orlando.

Furthermore, access to sites that overlook DoD assets highlights potential encroachment concerns. Private property and foreign land purchases could offer observation points for FIE collectors or other malicious actors. For instance, Blackstone called off the sale of the Hotel del Coronado to China's Anbang Insurance Group in 2016 following concerns raised by the Committee on Foreign Investment in the United States (CFIUS) and other national security officials, as the hotel is located on the same peninsula as Naval Base Coronado. According to DoD officials, similar sites near DoD bases could offer surveillance opportunities against DoD test and training activities.

Sources

https://www.cbs8.com/article/news/local/san-diego-live-webcams-turned-off/509-a330e6c9-8670-4486-8e58-5a54d216b008

https://www.navytimes.com/news/your-navy/2023/04/19/popular-san-diego-web-cameras-removed-at-navys-request/

https://news.usni.org/2023/04/13/swift-actions-by-jos-prevented-warship-collision-in-san-diego-harbor-investigation-finds

https://www.dcsa.mil/Portals/91/Documents/CI/2022_CI_Targeting_US_Technologies.pdf

https://www.wsj.com/articles/army-rips-out-chinese-made-surveillance-cameras-overlooking-u-s-base-1515753001

https://www.gao.gov/products/gao-15-149

Unsolicited Smartwatches Sent to Servicemembers – *Foreign Intelligence Entities (FIE)*

Summary

In mid-June, Army Criminal Investigations Division (CID) officials reported that several servicemembers had received smartwatches in the mail that they did not order. When turned on, the smartwatches connected to a wireless internet signal automatically and collected cell phone data, unprompted. These smartwatches are being treated as cybersecurity concerns, as there is a possibility they could collect sensitive information, such as banking records, contacts, and account usernames and passwords. The Army CID announcement did not state the origin or the senders of the unsolicited smartwatches, and the motive for mailing the devices is unknown. Whether the smartwatches are an attempt at espionage or brushing (when companies send unsolicited products to boost online reviews) the situation is being treated as a potential hazard due to the associated security risks. Army CID officials urge the use of caution to those who receive the smartwatches, recommending that

individuals not turn on the device and report them to the unit security or counterintelligence manager.

Analyst Comment

Foreign adversaries are constantly developing new methods to collect intelligence and disrupt U.S. domestic and foreign activities. "Smart" technology and networked devices have been at the forefront of these methods because of their omnipresence and users' reliance on them to carry out daily tasks and operations.

A similar event occurred in 2008 when an infected USB flash drive from an unknown source was picked up by a DoD employee and plugged into a laptop connected to CENTCOM. Malware spread to systems throughout the DoD, leading to 14 months of cleanup. The use of smartwatches is no different, and foreign intelligence entities may use them to gather information on logistics, operations, personnel and asset movement, and other mission-critical information. In a 2017 incident, Strava data revealed the locations of military installations throughout multiple countries, from Syria and Afghanistan to the highly classified Nevada Test and Training Range in the U.S. This data, when combined, could be used to reveal the identities of servicemembers in classified operations and locations.

Sources

https://www.jbsa.mil/News/News/Article/3429534/cyber-hygiene-cid-lookout-unsolicited-smartwatches-received-by-mail/

https://www.securityweek.com/us-military-personnel-receiving-unsolicited-suspicious-smartwatches/

https://www.bbc.com/news/technology-42853072

https://www.theguardian.com/world/2018/jan/28/fitness-tracking-app-gives-away-location-of-secret-us-army-bases

https://www.computerworld.com/article/2514879/infected-usb-drive-blamed-for--08-military-cyber-breach.html

https://www.foreignaffairs.com/articles/united-states/2010-09-01/defending-new-domain

Phishing Attacks Using New Top-Level Domains – *Cyber*

Summary

Google recently released eight (8) new top-level domains (TLD's) including .dad, .exq, .prof, .phd, .nexus, .foo, .zip, and .mov. The new domains are now open to the public and are available for purchase. The latter two (2) have a risk of misuse by threat actors in phishing attacks.

The concern is that Zip archives and MPEG-4 videos use the file names .zip and .mov, respectively. As such, clicking on both types of files is routine in some occupations, increasing the potential for successful phishing attacks.

Furthermore, some messaging platforms and social media platforms will automatically convert .zip and .mov file names into URLs now that they are also TLDs. A threat actor could post instructions on how to extract a .zip file or open a .mov video to watch. The target would open a link to a .zip domain owned by the threat actor, possibly downloading malware. It is unlikely that threat actors will create a significant number of domains to catch victims. However, a targeted attack only requires a single user to fall for the scam and affect an entire network. Unsuspecting servicemembers or their families could become victims of a phishing attack, putting DoD networks and their personal data at risk.

Analyst Comment

Malicious actors are fast to exploit emerging vulnerabilities. Cyber intelligence firm Silent Push Labs has already discovered what appears to be a phishing page attempting to steal Microsoft Account Credentials using the .zip domain. DoD personnel and their families are often targets for scams. Many young servicemembers are away from home and earning their own pay for the first time. This makes them potential targets. Servicemembers also move often, requiring changes in personal accounts such as banking, utilities, and insurance. This entails emails and communications from new sources that may be exploited. Servicemembers are also trained to follow orders. Threat actors prey on this and send emails that appear official and direct, creating a sense of urgency. There have been many scams in recent years targeting DoD personnel and their families.

Proper and continuous training on cybersecurity awareness should begin early in a servicemember's career and should include dependent family members. Cybersecurity changes rapidly. Those unaware of recent developments are more likely to fall for new scams. Awareness of the new .zip and .mov TLDs and strict adherence to established cybersecurity best practices can help mitigate these attacks.

Sources

https://thehackernews.com/2023/05/dont-click-that-zip-file-phishers.html

https://www.army.mil/article/71293/phishing_scams_target_military_families_veterans

https://www.defense.gov/News/News-Stories/Article/article/1921988/these-social-media-scams-affect-the-military/

Russian Ransomware Gang Hacks File Transfer Program – *Cyber*

Summary

In June, the "Cl0p" ransomware gang hacked the U.S. Department of Energy (DOE), private sector companies, and other state and federal agencies through a vulnerability in the file transfer program MOVEit. The files held crucial financial and insurance data for the past years and for future projects for these companies. State offices, such as the Louisiana Office of Motor Vehicles and the Oregon Department of Transportation, were also hacked, exposing the personal identifying information (PII) of private citizens, including residential addresses and social security numbers. Open-source information indicates that 2,500 "MOVEit" servers were vulnerable. Of these servers, 790 were international corporations, and 200 were government agencies. Past Cl0p attacks include the 2023 attack on GoAnywhere servers, which affected 130 corporations and the 2020 and 2021 attacks on the Accellion File Transfer Application devices, which impacted the Reserve Bank of New Zealand, Australian Securities and Investments Commission, and the Office of Washington State Auditor.

Analyst Comment

Hackers stealing the PII of American citizens through ransomware attacks could potentially reveal DoD servicemembers' data and other valuable information. Open-source research indicates that servicemembers are about 22% more likely to report that their stolen information was misused to open a new account, especially for credit cards. Additionally, the Federal Trade Commission noted that 20% of reports from active-duty servicemembers indicate that they have already experienced two (2) or more types of identity theft.

Using state-sponsored (or state-sanctioned) ransomware gangs, Russia has attempted to gain an edge by attacking Western cyber architecture. They seek vulnerabilities that they can exploit for both financial gain and actionable intelligence for the Kremlin. The connection between Western governments and the private sector is often a target. For example, during the June 2017 "NotPetya" hack, Russian military hackers attacked a Ukrainian software update that held intelligence information from the U.S., UK, and EU authorities. All told, the incursion caused $10 billion in damage and was the costliest cyberattack in history. Furthermore, in 2021, 74% of ransomware attacks globally were committed by Russian-backed hackers. Ultimately, more than $400 million of crypto payments went to gangs affiliated with the Russian government.

Sources

https://apnews.com/article/hack-ransomware-extortion-moveit-cisa-0a642dd9b3544552d8802befec6de9af

https://www.bbc.com/news/technology-60378009

https://www.wired.com/story/notpetya-cyberattack-ukraine-russia-code-crashed-the-world/

https://www.bbc.com/news/technology-60841924

https://www.gao.gov/products/gao-23-105084

https://www.theguardian.com/technology/2023/jun/16/moveit-transfer-hack-department-of-energy

https://www.usatoday.com/story/news/politics/2023/06/15/cyberattack-spree-breaches-us-agencies/70326695007/

https://techcrunch.com/2023/03/22/fortra-goanywhere-ransomware-attack/

https://www.bleepingcomputer.com/news/security/global-accellion-data-breaches-linked-to-clop-ransomware-gang/

Missing 14-Year-Old Girl Found at Camp Pendleton – *Crime*

Summary

A 14-year-old California girl who had been missing for weeks was discovered in the barracks room of a Marine at Camp Pendleton. The girl was reported missing by her grandmother in mid-June, after which a deputy from the San Diego County Sheriff's Department took a report. At the time of her disappearance, the girl's information was entered into missing person databases, which informed other law enforcement agencies of her disappearance. The girl left home a few days prior. Open-source reporting suggested that the girl has a learning disability and a history of running away from home. Two (2) Navy corpsmen found the girl wandering around the barracks. The duty logbook showed that she was discovered around 0900 and remanded to a separate location within 30 minutes. NCIS agents arrived shortly thereafter. She was at Camp Pendleton for about 24 hours. While investigators are examining the possibility that the girl was a victim of human trafficking, NCIS and other investigating agencies have, thus far, been unable to find evidence thereof. Both the Marine and the girl stated that they met on a dating app, where the girl used a pseudonym and claimed to be 22 years old. They reportedly had sexual contact in his barracks room. The Marine was and is cooperating with the investigation. He willingly furnished all of the data from his cell phone, including messages in which the victim admitted to lying about her age. He has been released to his command pending further investigation. Thus far, there have been no charges and no arrests. The girl reportedly told investigators that she was being trafficked by a pimp, but there was no evidence to support her claim. However, the investigation is ongoing.

Analyst Comment

The use of online dating apps poses unique risks to servicemembers. The U.S. Department of Justice has warned federal employees about the volume of personal information collected by these services, including users' sexual preferences, HIV status, pictures, phone number, private messages, location, and times of day the app is accessed. The intimate details that users willingly provide could, in some cases, be useful to threat actors. Open-source media demonstrates that these services are already used by criminals to facilitate robbery and sexual assault. However, servicemembers also have access to DoD facilities, assets, and systems. Personal information and compromising images and texts could easily be used by foreign intelligence entities and criminals for blackmail or to recruit insider assets. Servicemembers may also become unwittingly involved in criminal activity or be coerced into participating. The subsequent arrest and investigation of personnel has a substantial and negative impact on individual units, their chains of command, and the larger services. NCIS strongly advises personnel to be cautious about sharing personal details and media online, whether on dating apps or social media.

Sources

https://www.military.com/daily-news/2023/07/11/14-year-old-girl-found-pendleton-barracks-may-have-met-marine-tinder-new-documents-show.html

https://ktla.com/news/california/14-year-old-girl-found-in-barracks-at-camp-pendleton-what-we-know/

https://ktla.com/news/local-news/family-of-missing-young-girl-found-at-camp-pendleton-says-she-was-raped/

https://www.nbcnews.com/tech/security/dating-apps-grindr-could-pose-national-security-risk-experts-warn-n1115321

https://abc7chicago.com/lawndale-chicago-armed-robbery-dating-app-its-just-lunch/13213016/

https://www.ncis.navy.mil/Portals/25/Documents/Media/NCIS%20Sextortion%20Brochure_V2.pdf

---

Memorial Day Shooting in Hollywood, Florida – *Active Shooter*

Summary

On Memorial Day 2023, after an altercation between two (2) groups on the Hollywood Oceanfront Boardwalk 20 miles north of Miami, shots were fired, injuring nine (9) people. Four (4) of the victims were children, and all victims' ages ranged from one (1) to 65. While nine (9) people were hit, seven (7) were bystanders. Two (2) of the wounded were each part of a group involved in the shooting. A police affidavit stated that multiple individuals from a group drew firearms and shot not only at the other group, but also towards innocent bystanders.

After the shooting, investigators found five (5) handguns, two (2) of which were stolen. As of early June, five (5) suspects have been arrested. Three (3) of the five (5) arrested were 18 years old or younger. All three (3) were charged with one (1) count of attempted first-degree murder, eight (8) counts of attempted second-degree murder, and one (1) count of carrying a concealed firearm.

Analyst Comment

From 2014-2019, the U.S. has never experienced year with more than 417 mass shootings. The year 2014 recorded 273 mass shootings, 2015 recorded 336, 2016 had 383, 2017, had 348, 2018 had 336, and 2019 had 417. The year 2020 recorded 610, 2021 recorded 690, and 2022 had 647 mass shootings. As of mid-July, there were 374 mass shootings. This year is on track to reach more than 600 mass shootings. The reasons for the increase are multifaceted. Debates on how to reduce the overall number continue between lawmakers and voices in open-source media.

The Naval Surface Warfare Center Carderock Division's South Florida Ocean Measurement Facility is located in Fort Lauderdale, Florida and has been in operation for more than 50 years. DoD personnel are just as likely to be injured or killed in an active shooter event as their civilian counterparts. While the shooters at the Memorial Day incident were not targeting servicemembers, mass shootings in and around DoD installations could potentially affect personnel transiting to and from installations or while on leave or liberty.

Sources

https://www.gunviolencearchive.org/

https://www.cnn.com/2023/06/05/us/florida-hollywood-beach-shooting-arrests/index.html

https://abcnews.go.com/US/cities-us-rocked-memorial-day-weekend-shootings/story?id=85083526#:~:text=Cities%20across%20US%20rocked%20by%20Memorial%20Day%20weekend,4%20people%20shot%20in%20Memphis%20...%20More%20items

https://www.bbc.com/news/world-us-canada-41488081

https://www.navsea.navy.mil/Home/Warfare-Centers/NSWC-Carderock/Who-We-Are/Fort-Lauderdale-Florida/

Animal Sedative Xylazine Being Mixed with Fentanyl – *Narcotics*

Summary

The Biden Administration recently declared that the ongoing opioid crisis, heavily impacted by the use of fentanyl, is now an "emerging threat" to the U.S. As of late, fentanyl has been found with xylazine, which is an animal tranquilizer that is used to sedate horses, cattle, and other mammals, specifically for anesthesia, muscle relaxation, and analgesia.

The U.S. Drug Enforcement Administration (DEA) has seized mixtures of xylene and fentanyl in 48 of 50 states. In 2022, approximately 23% of all fentanyl powder confiscated by the DEA contained xylazine. Approximately 7% of fentanyl pills contained xylazine. The Center for Disease Control (CDC) has reported that between August 2021 and August 2022, 107,735 Americans died from drug overdoses. Of those deaths, 66% (71,105) involved synthetic opioids like fentanyl.

Analyst Comment

While the use of illicit opioids seems to be growing, the Office of National Drug Control Policy has released a six-point plan to scale increase testing, establish treatments, and intercept and disrupt illegal shipments of xylazine. The White House and the DoD have made efforts to fight this crisis, but with numbers rising at an unprecedented rate, the challenges of intercepting illegal shipments is ongoing. The combination of xylazine and fentanyl is often called "tranq" among dealers and users and has been referred to as a "zombie drug" in open source. It lowers the user's heart rate and blood pressure to unsafe levels and causes deep ulcers on the skin. It also makes it more difficult to use naloxone (brand name Narcan) to reverse an opioid overdose, as there is no antidote for xylazine poisoning.

While the White House has begun to act on the crisis, the DEA released a report in October 2022 to highlight just how fast the use of xylazine and other illicit opioids had grown. From 2020-2021, the U.S. saw dramatic increases in the laboratory identifications of xylazine by region. In the Northeast, there was an increase from 346 to 556 (61%) identifications by the DEA. The South saw a rise of 193%, from 198 to 580. The Midwest recorded less of an increase from other regions, sitting at just a 7% rise, from 110 to 118. The West increased from 77 to 163 (112%) from 2020-2021. In addition to the rise in laboratory identifications, the DEA has also recorded a rise in xylazine-related deaths. From 2020-2021, deaths in the Northeast increased from 631 to 1,281 (103%). The South recorded a 1,127% rise in xylazine-related deaths, from 116 to 1,423. The region led all other U.S. regions by at least 150 deaths. The Midwest increased from 57 to 351 (516%) deaths. The West had the least number of deaths in the timeframe, but the number still increased by 750%, from four (4) to 34.

Sources

https://abcnews.go.com/US/wireStory/white-house-lays-effort-animal-sedative-xylazine-call-101074961

https://www.cnn.com/2023/04/12/health/fentanyl-xylazine-emerging-threat-us/index.html

https://www.dea.gov/alert/dea-reports-widespread-threat-fentanyl-mixed-xylazine

https://www.dea.gov/sites/default/files/2022-12/The%20Growing%20Threat%20of%20Xylazine%20and%20its%20Mixture%20with%20Illicit%20Drugs.pdf

Hazards

Hurricane Season Outlook and Preparation– *Meteorological Hazards (Tropical Cyclones)*

Summary

The National Oceanic and Atmospheric Administration (NOAA) has predicted that this year's hurricane season will see near-normal activity. The forecast calls for 12 to 17 named storms (39 mph or higher winds). Five (5) to nine (9) could become hurricanes (74 mph or higher winds) with one (1) to four (4) of those hurricanes reaching major hurricane status (111 mph or higher winds). Conditions guiding this prediction are the expected El Niño to develop this summer, which hinders hurricane activity. However, an expected West African monsoon season with above-average sea surface temperatures in the Atlantic Ocean will promote hurricane activity. These offsetting conditions lead forecasters to the conclusion that there will be average hurricane activity this year. Since the start of Hurricane Season 2023 in June, three (3) named storms have developed, with two (2) in the Atlantic Ocean and one (1) in the Gulf of Mexico.

Hurricane season has the potential to affect DoD facilities and operations. There is an active training schedule during the summer, especially for reserve units. The Navy and Air Force use several locations with special use airspace across the Gulf of Mexico and Atlantic Ocean for aerial combat training. Many Army and Marine Corps training grounds are also located near coastal areas. The most concerning impact is a hurricane striking a coastal DoD installation. Recent examples include Hurricane Sally striking Naval Air Support (NAS) Pensacola in 2020, causing an estimated $450 million in damage. Tyndall Air Force Base (AFB) was struck by Hurricane Michael in 2018, causing an estimated $25 billion in damage. NAS Pensacola was not mission capable for 36 hours following the Category 2 storm. Tyndall AFB as struck by a Category 4 storm and suffered catastrophic damage that required years of recovery and rebuilding.

Analyst Comment

Hurricanes are, by their nature, unpredictable. Though analysts may project their tracks days or even weeks out, they can still shift course or gain strength shortly before landfall. There is a tendency to prepare for what a storm is expected to do rather than prepare for the worst-case scenario. In the case of NAS Pensacola, aircraft were not relocated. In hindsight, installation leadership stated that the aircraft should have been moved to other installations.

Installations should be conducting Hurricane Exercises (HUREX) to test preparedness of equipment and to train servicemembers who may be experiencing their first Hurricane Season. These exercises are more effective when coordinated with local authorities, non-governmental organizations (NGOs), and National Guard units. Hurricane response efforts can easily require a whole-of-government approach for recovery. Individual servicemembers can prepare themselves and their families by following guidance from FEMA, local emergency managers, and their own installation leadership.

Sources

https://www.noaa.gov/news-release/2023-atlantic-hurricane-season-outlook

https://www.pnj.com/story/news/2020/09/21/how-nas-penscola-recovering-hurricane-sally/5846188002/

https://www.tyndall.af.mil/News/Article-Display/Article/2961406/surviving-hurricane-michael-in-building-909/

https://www.ready.gov/hurricanes

Heat Warnings and Advisories in Southern U.S. – *Meteorological Hazards (Extreme Heat)*

Summary

In late June, almost 40 million people were under excessive heat warnings and heat advisories in the U.S. Last week alone, the heat index in parts of Arizona, New Mexico, Texas, and Louisiana was recorded at 120°F. In Texas, ERCOT, the Texas state utility operator, issued a Weather Watch until 30 June informing Texans of the higher electrical demand due to the extreme heat. Ultimately, open-source reports indicate that this summer, two-thirds (2/3) of North America are at risk of energy shortages due to increased demand. Among the four (4) states, dozens of DoD installations and facilities rely on the power grids for energy.

Analyst Comment

Per the National Weather Service (NWS), an excessive heat warning is issued if an area is expected to experience heat index values of 105°F or higher for at least two (2) days and nighttime air temperatures will not drop below 75°F. Blackouts resulting from extreme heat at DoD installations could cause transportation delays and communication challenges and pose a health risk to personnel. Furthermore, extreme heat events could delay outdoor training due to the higher likelihood of personnel experiencing heatstroke, heat exhaustion, and dehydration. In 2021, a total of 1,872 active component servicemembers (0.14%) were diagnosed with heat exhaustion, and 489 (0.04%) were diagnosed with heatstroke. Furthermore, in 2021, 114 (23.3%) heatstroke cases and 19 (1.0%) heat exhaustion cases were hospitalized. Among the hospitalizations, there were 324 total bed days for heatstroke and 40 total bed days for heat exhaustion. According to the DoD, with national average temperatures predicted to increase by a range of 3°F to 10°F by 2100, extreme heat's impact on population health could intensify.

Sources

https://www.msn.com/en-us/weather/topstories/extreme-heat-means-two-thirds-of-north-america-could-suffer-blackouts-this-summer/ar-AA1d41UL

https://www.hprc-online.org/physical-fitness/environmental-extremes/military-heat-flag-conditions-explained

https://health.mil/Military-Health-Topics/Health-Readiness/AFHSD/Reports-and-Publications

https://cleanpower.org/facts/wind-power/

https://blog.ucsusa.org/kristy-dahl/military-extreme-heat/

https://phc.amedd.army.mil/topics/discond/hipss/Pages/default.aspx

https://www.nasa.gov/feature/goddard/2021/the-climate-events-of-2020-show-how-excess-heat-is-expressed-on-earth

https://www.climate.gov/news-features/understanding-climate/climate-change-global-temperature

https://militaryembedded.com/radar-ew/thermal-management/conduction-cooling-advancements-complement-ultra-compact-servers-in-battle-versus-excessive-heat

https://www.reuters.com/world/us/us-midwest-danger-rotating-power-blackouts-this-summer-2022-06-03

https://www.cnet.com/home/energy-and-utilities/what-are-blackouts-heres-what-causes-them-and-why-theyre-so-dangerous/

https://www.cnn.com/2023/06/26/weather/heat-texas-records-south-monday/index.html

---

Space Weather Activity Increasing – *Space Weather*

Summary

In early July, NASA observed the peaking of an X1.0 solar flare that erupted from a sunspot about seven (7) times the width of the Earth. Open-source reporting indicates that radiation from the flare ionized the top of Earth's atmosphere, causing a deep shortwave radio blackout over western parts of the U.S. and Pacific Ocean. Solar flares develop when magnetic fields surrounding sunspots become tangled, break, and then reconnect. According to NOAA, X-class flares can result in "strong" or "severe" disruptions, as they are 10 times the strength of M-class flares and 1,000 more powerful than B-class flares.

In some cases, such as the July incident, coronal mass ejections (CMEs) accompany long-lasting flares. CMEs, or large expulsions of plasma and magnetic field from the Sun's corona, directed toward Earth, can reach the planet in several days or as little as 15 to 18 hours. CMEs do not directly threaten human life. The Earth's magnetosphere and atmosphere form a barrier that deflects and prevents CME particles from hitting the planet's surface, but they can impact electricity supplies and cause satellite failures. Following the July incident, NOAA reported that imagery detected a partial halo CME, with a likely Earth-directed component.

Additional analysis into the CME led NOAA issue a G1 Minor Storm Watch a few days later, in which it was indicated that G2 storm levels could develop if more favorable conditions were observed.

Open-source reporting indicates that solar activity has increased in recent months. Within Solar Cycle 25, NWS predicted peak sunspot activity for 2025. Furthermore, the 11-year cycle was predicted to have "fairly weak" overall activity. However, in June, researchers noted that the cycle ramped up much faster than expected, with more sunspots and eruptions than initially forecasted. Ultimately, the Sun produced 160 sunspots in June, the highest monthly number since 2002. Some experts predict that the peak of Solar Cycle 25 could arrive in one (1) year, in which the Sun could be on a trajectory of producing just under 200 monthly sunspots.

Analyst Comment

DoD installations, particularly those utilizing satellite systems, can be impacted by solar activity. According to open-source information, CMEs causing G1 geomagnetic storms may cause fluctuations in the power grid and impact the accuracy of GPS and GNSS satellite navigation systems. For instance, while GPS systems often provide position information with an accuracy of a meter or less in calm conditions, severe space weather storms may cause errors that are tens of meters or more. In addition, solar flares and the particles from CMEs also could increase the drag on satellites in orbits near Earth. As a result, the satellites could burn up after spiraling inwards when re-entering the atmosphere. For example, Space X lost a fleet of more than 40 Starlink mini-satellites in this fashion when their launch occurred during a solar storm. Space weather events that cause failures and errors of satellites used by the U.S. military, such as those in the Defense Meteorological Satellite Program (DMSP), can impact the analysis of cloud, atmospheric, space weather, and Earth surface data for military operations. Furthermore, partial or system-wide blackouts resulting from space weather events can affect DoD strategies, communications, and aircraft operations.

Sources

https://www.cbsnews.com/news/sun-unleashes-powerful-solar-flare-radio-blackouts-earth/

https://www.space.com/sun-solar-flare-radio-blackouts-earth-july-2023

https://www.livescience.com/what-are-coronal-mass-ejections

https://www.livescience.com/space/the-sun/solar-maximum-could-hit-us-harder-and-sooner-than-we-thought-how-dangerous-will-the-suns-chaotic-peak-be

https://www.spaceweather.gov/news/what-coronal-mass-ejection-cme

https://www.swpc.noaa.gov/impacts/space-weather-and-gps-systems

https://www.ibtimes.com/geomagnetic-storm-may-impact-earth-this-friday-following-fourth-july-coronal-mass-ejection-3703592

https://www.swpc.noaa.gov/impacts/electric-power-transmission

https://www.swpc.noaa.gov/news/g1-minor-storm-watch-issued-07-july-2023

https://www.armytimes.com/news/your-army/2022/08/18/army-hands-satellite-missions-over-to-space-force/

https://www.spaceforce.mil/About-Us/Fact-Sheets/Article/2197779/defense-meteorological-satellite-program/

https://www.space.com/sun-highest-sunspot-number-since-2002

On the Radar

- **Artificial Intelligence Competition on the Rise.** *Nations are turning to artificial intelligence (AI) technology to maintain a competitive edge militarily, economically, and politically. Practical applications for AI grow everyday whether, related to the latest military advancements, creating efficiency in supply chains, or rapidly combing through imagery and data. AI will continue to have significant implications across the political, military, and economic spectrum and change the landscape of risk analysis.*
- **Military Vehicle Crashes into Building at Fort Stewart.** *In mid-July, a former Army Soldier took a Humvee from a motor pool on Fort Stewart and crashed the vehicle into the front of the 3rd Infantry Division's headquarters building. According to reports, the glass entrance to the building was destroyed, but there were no injuries. The Army veteran was taken into custody and charged with theft and destruction of government property. Army investigators and Fort Stewart officials have not announced a motive for the incident. The investigation is ongoing.*
- **Corporate Purchases of Agricultural Land in California.** *State and federal officials have raised concerns about a series of land purchases in Solano County, California (in close proximity to Travis Air Force Base) by an investment firm with unclear ownership. The firm, known as Flannery Associates LLC, was founded in 2018 in Delaware. A lawyer for Flannery Associates stated that the firm is majority American-owned, with the remaining 3% of invested capital originating from Ireland and Britain. However, it is unknown whether these claims are accurate, and it is possible that adversarial foreign actors could still be involved by proxy. Chinese and Iranian actors have previously utilized front companies as part of their espionage efforts.*