Washington State Fusion Center
INFOCUS
THURSDAY – 4 NOV 2021

	International	National	Regional and Local
Events, Opportunities Go to articles	11/04 China doubles-down on zero-Covid 11/04 Russia another Covid daily death record 11/04 WHO Europe chief concern: Covid rebound 11/04 India celebrates Hindu festival of lights 11/04 Netherlands reports bird flu outbreak 11/03 Germany: pandemic of unvaccinated 11/03 Ukrainians protest against vaccination 11/03 WHO authorizes India vaccine Covaxin 11/03 WHO urges countries hold off on boosters 11/03 Greece tightens restrictions unvaccinated 11/03 Europe Covid cases rise 5th straight week 11/03 UK official: hard months ahead Covid rates 11/03 Russia Covid surge shows no signs abating 11/03 Covid-19 does not infect human brain cells? 11/03 CSIS: Covid most disruptive event post-9/11 11/03 Ethiopia leader defiant as rebels advance 11/03 Study: Russia implicated in Ukraine conflict 11/03 China advice spark speculation Taiwan war 11/03 Iran sets date to resume nuclear talks 11/03 Iran seizes oil tanker; ownership dispute? 11/03 Maldives faces dire climate change threat 11/03 Climate summit: phase out coal-fired power	11/04 US surpasses 750,000 Covid deaths 11/04 Covid boosters same as original vaccines? 11/04 FAA can't prosecute violent travelers 11/03 Benefits denied to unvaccinated deaths 11/03 NYC mayor: young children vaccination 11/03 Covid shots young children begin Texas 11/03 Air Force hits vaccine deadline: 97% vax 11/03 Colorado hospitals nearly full; virus wave 11/03 Vaccinations for millions eligible children 11/03 Workers quitting in record numbers 11/03 Hawaii holds on to virus restrictions 11/03 Nursing school applications increase 11/03 Logistics woes: truck driver shortage 11/03 Alaska: ignore federal vaccine mandates 11/03 Minneapolis vote on police reform 11/03 Candidates of color make election history 11/03 Men behind vast majority of gun violence 11/03 Payments to separated migrants rejected 11/03 Fed steps toward end pandemic measures 11/03 Expert: gas prices stable 'for time being 11/03 CBO: citizenship path for illegals $500B 11/03 Pentagon details China info war on US 11/03 China military consistently beats estimates 11/03 Pentagon: China 1,000 nuke warheads 2030 11/03 Recall: Tastykake cupcakes	11/03 Unvaccinated and unemployed 11/03 DOH: 733,535 cases, 8727 deaths 11/03 Vaccine rollout for children begins 11/03 Lawsuit filed over death in CHOP zone 11/03 Seattle mayor: death threats, extremism 11/03 Ex-SPD chief Best on short list lead NYPD? 11/03 Sound Transit reduces trips, service hours 11/03 Set clocks back Sunday
Cyber Awareness Go to articles	11/04 GitLab servers exploited in DDoS attacks 11/03 BlackMatter moves victims to LockBit 11/03 UK Labour party hit by 'cyber incident' 11/03 Foreign tech firms pulling out of China 11/03 Stealthier version Mekotio banking trojan 11/03 France: Lockean in attacks on companies 11/03 Scanning web uncover malware infections 11/03 Mobile phishing attacks energy sector rise 11/03 'Tortilla' wraps Exchange servers in attacks 11/03 Twitter misinformation backed Kenya leader	11/04 Justice Dept. cyber crackdown 11/03 CISA new directive for patching 11/03 US blacklists NSO Group over spyware 11/03 Report: cost of breach in energy, utilities 11/03 Sinclair broadcasting ransomware attack 11/03 Holiday shopping: retail bot attacks surge 11/03 QR codes offer scammers another avenue 11/03 Official: unknown if Russia cracking down 11/03 Beware: Steam Discord free Nitro phishing 11/03 US hijacks ransom site; group shuts down 11/02 Hoax: 'Groove' ransomware gang 11/02 Owner of huge, leaked VPN database? 11/02 Ransomware operations continue to evolve	
Terror Conditions Go to articles	11/04 Taliban leader: infiltrators within ranks 11/03 AQ doubles down hatred on Jews, Israel 11/03 IS stepping up attacks east, central Syria 11/03 EU terrorism training Mozambique troops 11/03 ISIS growing threat to Taliban government	11/04 Radicalization's path: cases similarities 11/03 FBI declassifies 9/11 documents 11/03 Calif. man jailed 25yrs: bombing plot 11/03 FBI: equal threats domestic extremists, IS 11/03 Investigation into 'mistake' 29 Aug airstrike	
Suspicious, Unusual Go to articles	11/04 NKorea can make more uranium for bombs 11/03 Study: why world is protesting so much 11/03 Arctic warms: forecasting shifting sea ice 11/03 Globe bounces back to 2019 carbon levels	11/03 Report: 18 billionaires got stimulus checks	11/03 Report: cannabis is state's 4th valuable crop 11/03 Another Oregon county looks to join Idaho 11/03 Widow: 'where's the body' public autopsy?
Crime, Criminals Go to articles	11/04 Venezuela faces landmark ICC investigation	11/04 Philadelphia bans pretextual traffic stops 11/03 Judge: Arbery trial jury makeup stands 11/03 OECD: counterfeit products flood internet	11/03 Lakewood police investigate explosion 11/03 Tacoma police: man found shot in vehicle 11/03 Federal Way police homicide investigation

DISCLAIMER and FAIR USE Notice

Events, Opportunities

Top of page

HEADLINE	11/04 FAA can't prosecute violent travelers

SOURCE	https://www.cnn.com/2021/11/04/politics/faa-unruly-passengers-doj/index.html
GIST	**(CNN)**The Federal Aviation Administration -- which cannot prosecute violent airline passengers -- has sent only 37 of the more than 5,000 passenger complaints this year to the Justice Department, highlighting a significant challenge when it comes to enforcing the strict rules for the increasingly unruly skies. The FAA said it has sent the "most egregious cases" to the Justice Department. In a rare joint statement issued first to CNN, the two agencies said they are "working closely together to ensure unruly airline passengers face criminal prosecution when warranted." The multi-agency announcement comes after months of pressure from airline worker unions for the federal government to get tougher on violence on commercial flights. Flight crews have reported 5,033 such incidents so far this year, and the FAA has initiated enforcement action in 227 cases. "Where the evidence supports criminal review, the FAA refers the cases to the FBI," the joint statement said. The Transportation Security Administration also unveiled a new public service announcement on Thursday, highlighting an FAA letter referring a case to the Justice Department and outlining an actual fine issued. "You don't want this letter," the ad says, hoping to deter bad behavior. But unions underscore that in many cases, passengers walk free. The FAA does not have the power to prosecute criminal cases, only to assess civil fines up to $37,000. "I think we're making good progress, but there's certainly more to be done," FAA Administrator Steve Dickson said Wednesday at a hearing before the Senate Committee on Commerce, Science and Transportation. "It really does require the cooperation of all those private-sector stakeholders and including the airports, as well as the various aspects of the federal government." President Joe Biden said in early October that he has instructed the Justice Department to address the rising violence on airplanes as passengers resisting mask requirements threaten airline staff. "I instructed the Justice Department to make sure that we deal with the violence on aircraft coming from those people who are taking issues," Biden said during an October 7 event outside Chicago. "We're going to deal with that." On Monday, federal investigators charged Brian Hsu of Irvine, California, with assault and interfering with a flight crew, alleging he had punched an American Airlines flight attendant in the face. The charges could carry a 20-year prison sentence. Court documents detailing the October 27 incident say the flight attendant was trying to keep Hsu from reaching the lavatory while the seat belt sign was on. Hsu, who said he was traveling home following brain surgery, told investigators he was acting in self-defense.
Return to Top	

HEADLINE	**11/04 China doubles-down on zero-Covid**
SOURCE	https://www.cnn.com/2021/11/04/china/china-delta-covid-outbreak-strategy-intl-hnk/index.html
GIST	**Hong Kong (CNN)**China is scrambling to contain its most widespread Covid-19 outbreak since the first wave of infections that began in Wuhan in 2019. Though subsequent flare-ups have seen higher total case numbers, this outbreak has spread the furthest, with 19 of China's 31 provinces -- more than half the country -- reporting cases since the outbreak began in mid-October, according to the National Health Commission (NHC).

On Wednesday, the NHC reported 93 new symptomatic cases -- the highest daily count in three months. About 500 cases have been reported nationwide since the outbreak began, according to state-run tabloid the Global Times.

The number may seem small compared to other countries in the West, many of which are still reporting tens of thousands of cases each day. But it's massive for China, which has stuck to its "zero-Covid" approach, including tight border controls and lengthy quarantines for international arrivals.

This approach -- which aims to stamp out the virus completely within China's borders -- means even a handful of cases are viewed as a dire threat.

The ongoing outbreak began on October 16, when infections were detected among a tour group of fully vaccinated senior citizens from Shanghai traveling in northern China. Cases quickly ballooned and spread across northern provinces; by the following week, officials from the National Health Commission warned of "multiple scattered local outbreaks" in the north and northwest that were "expanding rapidly."

Authorities immediately jumped into action, following the playbook that has successfully contained previous outbreaks: mass testing, snap lockdowns, quarantines, travel suspensions and vigilant surveillance.

Officials banned cross-provincial tours across the affected regions. In one popular tourist destination, all residents and tourists were forbidden from leaving their homes. The capital Beijing tightened entry restrictions into the city, and punished rule-breakers by placing them in criminal detention.

Several cities, including Lanzhou, which has reported several dozen cases, have been placed under lockdown -- affecting millions of residents in total.

But the virus spread rapidly anyway, raising questions about the sustainability of zero-Covid -- as well as the efficacy of China's emergency responses, as outbreaks arrive more frequently for longer durations.

China's first-ever outbreak, at the start of the pandemic in Wuhan, had largely been brought under control by March 2020, with cases staying low for the rest of the year. Though there were occasional flare-ups, these were quickly contained as well; by the end of the year, much of daily life had returned to normal, with businesses in operation and domestic travel resumed.

But 2021 also brought the arrival of the highly infectious Delta variant, which has wreaked havoc around the world. Delta sparked severe outbreaks in many Asian countries that had, until then, contained the virus relatively well -- including Australia, Malaysia, Bangladesh, Thailand and Vietnam.

The more contagious variant, and the growing advice from international health experts that Covid would likely become endemic, has prompted many of those countries to abandon the zero-Covid approach, and instead adapt to "living with Covid."

In China, too, the effects of Delta are becoming clear. After its long stretch of relative normality, the country has recorded several outbreaks in the last few months alone, with little time in between to recover.

And concerns linger over the efficacy of Chinese vaccines, especially in face of the Delta variant. Close to 2.3 billion doses had been administered by Tuesday, and by late October 76% of the population had been fully vaccinated, according to the NHC -- but that hasn't stopped outbreaks from spreading fast and wide.

This summer, China experienced one of its most severe outbreaks yet, driven by Delta. The variant was first detected in July in the eastern city of Nanjing; soon, infections were being reported in dozens of cities and eventually spread to 16 provinces. After the familiar routine of mass testing, lockdowns, movement restrictions and mandatory quarantines, cases fell to normal levels by the end of August.

	Despite the apparent success, the summer outbreak took longer than previous flare-ups to contain -- and it had spread much faster between cities. Residents and authorities had only a few weeks to catch their breath before another outbreak emerged in September in Fujian province. This time, images of the government's stringent containment measures -- including separating children as young as four from their parents during quarantine -- drew international concern and criticism. By September 29, health officials declared that the Fujian outbreak had been brought under control. Less than three weeks later, the current outbreak emerged. However, despite the rising frequency and duration of its outbreaks, China shows no signs of changing its strategy -- even doubling down as it prepares for two high-profile events: a crucial meeting of Communist Party elites next week, then the Beijing Winter Olympics next February. "Faced with continued outbreaks of Covid-19, health experts believe China cannot abandon its zero-tolerance approach for now," said an editorial by Global Times on Wednesday, warning that "lifting the strict controls would lead to a catastrophic outcome."
Return to Top	

HEADLINE	**11/03 Expert: gas prices stable 'for time being**
SOURCE	**https://www.q13fox.com/news/gas-prices-stable-for-the-time-being-shouldnt-move-much-higher-expert-says**
GIST	Gasoline prices in the U.S. have stabilized "for the time being" and shouldn't move much higher as long as the price of oil holds, according to an industry expert. It may come as a relief for the nation which has been grappling with sky-high oil and gas prices, ultimately forcing the Biden administration to ask OPEC+ to help out America instead of going directly to U.S. oil producers. "As long as oil doesn't top $85, we shouldn't see the national average move much higher," Patrick De Haan, head of petroleum analysis for GasBuddy, told FOX Business. According to GasBuddy data, the national average is at about $3.39 per gallon. Meanwhile, the price of West Texas Intermediate crude oil dropped to $80.86 a barrel on Wednesday. "With WTI down so far this morning, we could see the national average start to trickle a little lower in the coming days," De Haan said. That is unless the price of oil spikes and with OPEC meeting Thursday to discuss oil output "we could see surprises there depending on the outcome," according to De Haan. In September White House Press Secretary Jen Psaki said the administration would "continue to speak to international partners, including OPEC, on the importance of competitive markets and setting prices and doing more to support the recovery." And in August, U.S. national security adviser Jake Sullivan said OPEC+'s rate of oil production increases was "simply not enough."
Return to Top	

HEADLINE	**11/03 Sound Transit reduces trips, hours**
SOURCE	**https://www.q13fox.com/news/sound-transit-to-nix-trips-reduce-service-hours-over-operator-shortages**
GIST	**SEATTLE** - Sound Transit is reducing service on express routes in Pierce and South King counties due to operator shortages.

	The transportation agency announced the service changes Wednesday, which will lead to the cancellation of trips, irregular schedules and occasional service delays. These changes officially take effect on Monday, Nov. 8: • **Route 566** is suspending some trips, including 'reverse peak' trips which run southbound in the morning rush hour and northbound in the afternoon rush. Sound Transit is also nixing some morning and evening rush hour trips. People are encouraged to use **KCM Route 160** and **ST Express 560** instead • **Route 577** is reducing some morning and evening rush hour trips, operating every 10–15 minutes. People are encouraged to use **KCM Route 177** • **Route 578** will have a minor adjustment to trip times • **Route 580** will only operate between Puyallup Station and South Hill P&R; Lakewood to South Hill P&R will be temporarily suspended, and Pierce Transit **Route 400** will replace some **Route 580** trips between South Hill P&R, Red Lot and Puyallup Station. Sounder trains will still have a timed connection at Puyallup Station • **Route 590** will reduce some trips during morning and evening rush hour to every 10–15 minutes • **Route 592** will reduce trips and change trip times • **Route 594** will have adjustments in trip times on weekdays Weekend service times will not be affected, Sound Transit says, and all other Pierce Transit routes—ST Express routes 560. 574, 586, 595 and 596—are unchanged, as well.
Return to Top	

HEADLINE	**11/04 Netherlands reports bird flu outbreak**
SOURCE	**https://www.reuters.com/world/netherlands-reports-bird-flu-outbreak-among-ducks-poultry-farm-2021-11-04/**
GIST	AMSTERDAM, Nov 4 (Reuters) - The Netherlands on Thursday reported a new outbreak of highly pathogenic H5 bird flu among ducks at a poultry farm in the central province of Flevoland. To limit the spread of the disease, about 10,000 animals will be culled at the farm, the Dutch agriculture ministry said. Commercial farms across the Netherlands last week were ordered to keep all poultry inside after an outbreak of bird flu was reported at a different farm in the region.
Return to Top	

HEADLINE	**11/04 WHO Europe chief concern: Covid rebound**
SOURCE	**https://apnews.com/article/coronavirus-pandemic-health-asia-geneva-pandemics-01edf6a054783f59dfbebf97a6de9bc3**
GIST	GENEVA (AP) — A 53-country region in Europe and Central Asia faces the "real threat" of a resurgence of the coronavirus pandemic in the coming weeks or already is experiencing a new wave of infections, the head of the World Health Organization's regional office said Thursday. Dr. Hans Kluge said case counts are beginning to near record levels again and the pace of transmission in the region, which stretches as far east as the former Soviet republics in Central Asia, is of "grave concern." "We are at another critical point of pandemic resurgence," Kluge told reporters from WHO Europe headquarters in Copenhagen, Denmark. "Europe is back at the epicenter of the pandemic, where we were one year ago." He said the difference now is that health authorities know more about the virus and have better tools to combat it. Relaxed prevention measures and low vaccination rates in some areas explain the latest surge, he said.

	Kluge said hospitalization rates due to COVID-19 in the 53-country region more than doubled over the last week. If that trajectory continues, the region could see another 500,000 pandemic deaths by February, he said. WHO Europe says the region tallied nearly 1.8 million new weekly cases, an increase of about 6% from the previous week, and 24,000 COVID-19 weekly deaths, – a 12% gain. Kluge said the countries in the region were at "varying stages of vaccination rollout" and that regionwide an average of 47% of people were fully vaccinated. Only eight countries had 70% of their populations fully vaccinated. "We must change our tactics, from reacting to surges of COVID-19, to preventing them from happening in the first place," Kluge said. WHO's headquarters in Geneva on Wednesday reported that cases had risen in Europe for the fifth consecutive week, making it the only world region where COVID-19 is still increasing. The infection rate was by far the highest in Europe, which reported some 192 new cases per 100,000 people. Several countries in Central and Eastern Europe have seen daily case numbers shoot up in recent weeks.
Return to Top	

HEADLINE	**11/04 Russia another Covid daily death record**
SOURCE	**https://apnews.com/article/coronavirus-pandemic-business-europe-pandemics-moscow-35a108358764a123be71ae772c17081a**
GIST	MOSCOW (AP) — Russia has set another record for daily coronavirus deaths as it struggles through a long surge of infections that has prompted restrictions throughout the country. The national coronavirus task force on Thursday said 1,195 people died of COVID-19 over the past day, exceeding the 1,189 recorded the previous day. Since late September, Russia has tallied new highs in infections or deaths almost daily. The task force reported 40,217 new infections, down from the record 40,993 on Oct. 31. Less than 35% of Russia's nearly 146 million people have been fully vaccinated against the coronavirus, even though Russia approved a domestically developed vaccine against the coronavirus months before most countries. Russia's state coronavirus task force has reported more than 8.6 million confirmed coronavirus cases and more than 243,000 deaths during the pandemic. Russia is six days into a nationwide nonworking period that the government introduced to curb the spread of the virus. Last month, President Vladimir Putin ordered many Russians to stay off work between Oct. 30 and Nov. 7. He authorized regional governments to extend the number of nonworking days, if necessary. Officials in Russia's Novgorod region, located 500 kilometers (310 miles) northwest of Moscow, said Monday that the time away from workplaces would last another week. Four other regions — the Tomsk region in Siberia, the Chelyabinsk region in the Ural Mountains, the Kursk and the Bryansk regions southwest of Moscow — followed suit Wednesday. The Smolensk region on the border with Belarus also extended the nonworking days, but only until Nov. 10. Governors of at least three other regions have said they were considering extending the nonworking period.

	In Moscow and the surrounding region, which together account for nearly 25% of new daily infections, the nonworking period won't be extended beyond Nov. 7, officials said. Certain restrictions will remain in place in the Russian capital, such as a stay-at-home order for older adults and a mandate for businesses to have 30% of their staff work from home. Access to theaters and museums is limited to those who either have been fully vaccinated, have recovered from COVID-19 within the last six months or can present a negative coronavirus test. But reports by Russia's state statistical service Rosstat that tally coronavirus-linked deaths retroactively reveal much higher mortality numbers than the task force's. A report released last week indicated that about 462,000 people with COVID-19 died between April 2020 and last September. Russian officials have said the task force only includes deaths for which COVID-19 was the main cause and uses data collected from medical facilities. Rosstat uses wider criteria for counting virus-related deaths and takes its numbers from civil registry offices where the process of registering a death is finalized.
Return to Top	

HEADLINE	**11/04 Covid boosters same as original vaccines?**
SOURCE	**https://apnews.com/article/coronavirus-pandemic-science-health-alabama-coronavirus-vaccine-507492229abfbc9b42d21d6de605e841**
GIST	NEW YORK (AP) — Are COVID-19 boosters the same as the original vaccines? Yes, COVID-19 boosters use the same recipe as the original shots, despite the emergence of the more contagious delta variant. The vaccines weren't tweaked to better match delta because they're still working well. The vaccines work by training your body to recognize and fight the spike protein that coats the coronavirus and helps it invade the body's cells. Delta's mutations fortunately weren't different enough to escape detection. The increased protection you might get from a booster adjusted to better match the delta or other variants would be marginal, says Dr. Paul Goepfert, director of the Alabama Vaccine Research Clinic at the University of Alabama at Birmingham. Manufacturing doses with a new formula would have also delayed the rollout of boosters. Moderna and Pfizer are studying boosters tweaked for the delta and other variants to be ready if one's ever needed. Health authorities would have to decide if and when a vaccine formula swap would be worthwhile. "What we don't know," Goepfert noted, "is if you have a delta vaccine compared to the regular vaccine, does it actually work better in preventing transmission or asymptomatic infection?" The U.S. has authorized booster doses of the Pfizer, Moderna and Johnson & Johnson vaccines for certain people, and a few other countries also are using boosters of those shots or other COVID-19 vaccines.
Return to Top	

HEADLINE	**11/04 US surpasses 750,000 Covid deaths**
SOURCE	**https://www.cnn.com/interactive/2020/health/coronavirus-us-maps-and-cases/**
GIST	Covid-19 has killed at least 750,431 people and infected about 46.3 million in the United States since last January, according to data by Johns Hopkins University. On a per capita basis, North Dakota, Alaska and Tennessee have reported the most cases while Mississippi and Alabama are leading the country in deaths.

	Those numbers fail to paint a complete picture, however, since testing scarcity and delays likely left many Covid-19 cases and deaths undiagnosed, especially during the outbreak's early stages. In fact, the Centers for Disease Control and Prevention estimate that as many as 1 in 3 people in the United States has been infected, more than three times the official count. The Food and Drug Administration (FDA) has authorized the use of vaccines from three manufacturers — Pfizer/BioNTech, Moderna and Johnson & Johnson — and a mass vaccination campaign is underway in the United States. While new daily cases have dropped dramatically from the January 2021 peak, the race between vaccines and variants continues, especially in parts of the country that are less vaccinated.
Return to Top	

HEADLINE	**11/03 Benefits denied to unvaccinated deaths**
SOURCE	**https://www.cnn.com/2021/11/03/health/unvaccinated-death-benefits-khn-partner/index.html**
GIST	(KHN)These days, workers who refuse to get vaccinated against covid-19 may face financial repercussions, from higher health insurance premiums to loss of their jobs. Now, the financial fallout might follow workers beyond the grave. If they die of covid and weren't vaccinated, their families may not get death benefits they would otherwise have received. New York's Metropolitan Transportation Authority no longer pays a $500,000 death benefit to the families of subway, bus and commuter rail workers who die of covid if the workers were unvaccinated at the time of death. "It strikes me as needlessly cruel," said Mark DeBofsky, a lawyer at DeBofsky Sherman Casciari Reynolds in Chicago who represents workers in benefit disputes. Other employers have similar concerns about providing death or other benefits to employees who refuse to be vaccinated. In Massachusetts, the New Bedford City Council sought to extend accidental death benefits to city employees who died of covid, but the mayor didn't sign that legislation because, among other things, it didn't prohibit payment if the worker was unvaccinated. President Joe Biden has leaned hard on businesses to make sure their workers are vaccinated. In September, the administration announced all employers with 100 or more workers would be required to either ensure they're vaccinated or test employees every week for covid. Among employers, "there's a frustration level, particularly at this point when these vaccines are fully approved," said Carol Harnett, president of the Council for Disability Awareness, an industry group. "You're trying to protect yourselves and your employees, both from themselves and the general public." The New York transportation authority is the highest-profile employer to take this action. Since the pandemic crisis began in 2020, 173 MTA workers have contracted covid and died. Five of those deaths occurred after June 1 of this year, when the policy changed, according to the MTA. "We are not aware they have been vaccinated," an MTA spokesperson said of the five workers who died since the policy took effect. The transit authority's policy was a shift from an earlier pact with workers. In April 2020, as covid ravaged New York, transit officials and the labor unions representing employees reached agreements that workers who died of covid would be eligible to receive a $500,000 lump-sum death benefit, just like payments to which families of MTA workers who have other job-related deaths are entitled. The program will continue through the end of this year.

But with covid vaccines now widely available and fully approved by the Food and Drug Administration, the MTA Board determined that, starting June 1, workers who died of covid had to have been vaccinated for their families to be eligible for the payment.

The change comes as the MTA has struggled to improve vaccination rates among its roughly 67,000 workers. More than 70% of transit employees are estimated to be vaccinated, according to MTA officials.

A spokesperson for the MTA stressed that the program remains in effect, and noted that it has been extended past its original one-year term. The only change is the vaccination requirement.

"The program is not being revoked," the MTA spokesperson said in an email. "In fact, the MTA has twice extended it."

Local 100 of the Transport Workers Union, which represents roughly 38,000 MTA workers, pushed hard to negotiate the benefit. "No other workforce in the city, probably the country, secured what TWU secured: a $500,000 payment from the employer to the families of workers who died after getting covid," said Pete Donohue, a union spokesperson. "We look at it that during a terrible time, we got [the benefit] for people."

It's not unusual for employers of workers in risky occupations — such as police, firefighters, utility company workers and transit workers, who could succumb to an industrial accident or get hit by a train on the tracks — to offer extra insurance coverage that pays if they die on the job. The coverage is often provided in addition to a regular life insurance policy.

These so-called line-of-duty or accidental death and dismemberment policies typically don't pay out if someone dies of a disease. How can it be proved that someone picked up a deadly infection at work rather than at the supermarket?

But with covid, some front-line workers have been considered eligible for accidental death benefits because they are presumed to have gotten sick on the job, DeBofsky said.

Workers may be denied death benefits, however, if they didn't follow established safety protocols, said John Ehrlich, the national lead consultant at Willis Towers Watson on group life insurance. Failing to wear a bulletproof vest, a helmet or other safety equipment, for example, might make their families ineligible for payment under a policy.

Now that vaccines are widely available, some employers have considered limiting other benefits paid to unvaccinated workers, including reducing short-term disability payments, said Rich Fuerstenberg, a senior partner at benefits consultant Mercer. But Fuerstenberg said he had not heard of other employers eliminating death benefits for unvaccinated workers.

In the New Bedford case, the City Council unanimously passed a petition in August stating the covid death of any city employee would be considered to have occurred in the line of duty, enabling family members to receive accidental death benefits.

Mayor Jon Mitchell, however, objected for several reasons — the question of vaccination among them.

"As I am certain the Council would agree, it would be inappropriate to extend accidental death benefits where the employee refused to take a vaccine that had been found to be nearly 100% effective," Mitchell said in a letter to the council. The proposal has been tabled for further negotiation, according to a spokesperson for the mayor.

For more than 17 years, Joseph Fletcher worked for the MTA in Brooklyn, doing body work and other maintenance on buses.

	When he died of covid on April 11, 2020, at age 60, he left behind his wife, Veronica, a former high school teacher who was disabled after a car accident, and three children, now 9, 13 and 16. Coping with his death was hard enough, but looking toward the future has been overwhelming, Veronica said. "How am I going to keep afloat financially?" she worried. "Everything about this journey is terrifying." The $500,000 death benefit helped cover the family's regular bills and pay the mortgage on their Brooklyn home. But she's aware it will go only so far, and her three children need to go to college. If the MTA vaccination requirement had been in place when her husband died, it wouldn't have been a problem, Fletcher said. "I wish that my husband were able to have been vaccinated," she said. "Knowing my late husband, he would have taken the opportunity to protect himself and his family."
Return to Top	

HEADLINE	**11/03 Hawaii holds on to virus restrictions**
SOURCE	**https://www.seattletimes.com/seattle-news/health/hawaii-holds-on-to-virus-restrictions-even-as-cases-plummet/**
GIST	HONOLULU — Hawaii remains among the most restrictive states for COVID-19 mandates, despite having one of the highest vaccination rates in the country. Various state and county rules have changed often, leaving some businesses, travelers and residents confused and frustrated. Hawaii Gov. David Ige said earlier this year that all restrictions would end once 70% of the population was fully vaccinated. But a surge of delta variant cases filled hospitals and extended rules to guard against COVID-19. Now, case counts have dropped and about 83% of eligible Hawaii residents are fully vaccinated. But many rules remain in place. Germaine Malabanan plans to get married on Oahu this month after her wedding was delayed twice because of the pandemic. Security guards that are required for weddings will make sure her guests are wearing masks even while outdoors, the Honolulu Star-Advertiser reported Monday. “If everyone is vaccinated and we are all outside, I don’t see why we need the masks,” Malabanan said. The rules also mean unvaccinated guests can’t come. While most venues on Oahu allow proof of vaccination or a negative COVID test for admission, regulations don’t allow weddings to use the testing option. “From what I understand, Hawaii has one of the best, if not the best, turnouts for the vaccine, and we are still one of the most restricted and shut-down places,” said Joseph Esser, a wedding photographer and president of the Oahu Wedding Association. The wedding rules are part of a complicated set of statewide and county restrictions. In early July, most U.S. states had scaled back mask and other coronavirus restrictions. The delta variant surge pushed some jurisdictions to reinstate rules, but many are again easing as cases currently plummet.

	Ige's latest 50-page emergency proclamation outlines the various measures. For example, passengers cannot ride in a private car without a mask unless everyone is a member of the same household or fully vaccinated. People are forbidden from mingling at restaurants and bars. And private indoor gatherings of more than 10 people are not allowed. "We look at many factors before implementing or reducing restrictions," Ige told the Star-Advertiser in a statement. "Large-scale gatherings could easily and rapidly result in the kind of surge that could force us to reinstate restrictions, which we would like to avoid." County rules can vary, and changes need clearance from the governor. On Oahu, Honolulu Mayor Rick Blangiardi announced last week that some restrictions will relax beginning Wednesday — but some people are still confused. Masks are not required for participants of outdoor marathons, but they are required for outdoor parties, weddings and funerals. No food or drinks are allowed at football games, but they are OK in movie theaters. To go to a concert, people must be fully vaccinated. But to go to a bar, patrons can show a negative COVID test. Peter Yee, a Maui car rental employee who was laid off last year, said the restrictions have been too harsh on workers. "People are exhausted from the restrictions," he said. "That's the vibe in Hawaii."
Return to Top	

HEADLINE	**11/03 Lawsuit filed over death in CHOP zone**
SOURCE	**https://www.kiro7.com/news/local/durkan-sawant-seattle-sued-death-chop-zone/UGJX6VAXJ5DJVGMEVL7RHMCHOM/**
GIST	SEATTLE — A lawsuit has been filed on behalf of Horace Anderson and the estate of his deceased son, Lorenzo Anderson, a 19-year-old who was shot near the Capitol Hill Occupied Protest zone. The lawsuit holds Seattle Mayor Jenny Durkan, City Council Member Kshama Sawant and the City of Seattle responsible for the death. CHOP was a seven-block, police-free protest zone that the mayor, City Council and other government entities allowed during the George Floyd protests. Lorenzo Anderson was shot in the early morning hours of June 20, 2020, on Pine Street, and Seattle medics refused to enter the CHOP zone because Seattle police could not secure the scene. A bystander took him to Harborview Medical Center, where he was pronounced dead. The lawsuit claims there are more than 2,400 pages of exhibits that provide evidence showing that actions and inactions by the defendants "were directly responsible for the chaos promoted and encouraged that lead to the wrongful and preventable death of (Lorenzo) Anderson." Attorney Evan M. Oshan said key exhibits include a reprimand of Sawant and more than 300 pages of invoices showing funds were mismanaged to promote the CHOP zone.

	A news release from Oshan said other exhibits show how Seattle medics and police officers were nearby and available to help the dying teen when 911 calls were received, but they failed to perform their duties "as a result of failed Seattle leadership." A federal wrongful death lawsuit was filed against the city in April this year on behalf of Anderson's mother, Donnitta Sinclair, but Oshan said it was dismissed this week.
Return to Top	

HEADLINE	**11/03 Unvaccinated and unemployed**
SOURCE	**https://thefalcon.online/11489/news/covid-19/unvaccinated-and-unemployed/**
GIST	As the pandemic continued to sweep across communities in Washington State, Governor Jay Inslee announced a statewide vaccine requirement for most state employees on Aug.18, resulting in some first responders to risk their employment instead of being vaccinated. In a statement made by Gov. Inslee, he issued the mandate to apply to state workers regardless of their teleworking status. "It is the mission of public servants and those providing health care to serve our fellow Washingtonians. These workers live in every community in our state, working together and with the public every day to deliver services," Inslee said. "We have a duty to protect them from the virus, they have the right to be protected, and the communities they serve and live in deserve protection as well." Since then, numerous individuals and legal groups have attempted to block this order from taking place. On Oct. 25, U.S. District Court Judge Thomas Rice declined to stop Gov. Inslee's mandate in court. "The Supreme Court has long endorsed state and local government authority to impose compulsory vaccines… Federal courts have routinely analyzed such cases using rational basis and regularly reject cases similar to this one that challenge vaccine mandates based on free exercise of religion," said Rice in his ruling. Rice explained that the reason for not blocking Gov. Inslee's mandate was that it was "well-supported by extensive medical evidence, recommendations by professional organizations, and aligns with other measures already in place in other governmental settings." Now, more than 170 Seattle Police and Seattle Fire first responders have been placed on leave as they await exemptions. The Seattle Police Department announced that 103 officers are currently awaiting exemption after six had their employment terminated. Kristin Tinsley, the Seattle Fire Department's public information officer, announced in a statement that as of Oct. 29, 94% of the city's 1,086 employees are vaccinated. "Fifty-five employees have submitted exemptions (48 religious, 7 medical) and are involved in the City's exemption and accommodation process. Seven employees did not submit either a vaccine verification form or exemption form. Of the seven, three have been separated, three are in the separation process, and one is retiring," said Tinsley. Faced with concerns about issues responding to calls in a timely manner as a result of the mandate, Tinsley said, "at this time, we are not experiencing significant response delays." The Seattle Fire Department has prepared a contingency plan that includes cancelling all non-essential training, community events and limiting annual building inspection focus to schools. The department also plans to prioritize which units could be placed out-of-service through an analysis of response routes to ensure city coverage by Seattle Fire Department remains in effect.

	The Washington State Patrol announced on October 19 that 127 individuals at the department had separated from employment as a result of the mandate. This consists of 53 civil servants and 74 commissioned officers (67 troopers, 6 sergeants, and 1 captain). Washington State Patrol Chief John R. Batiste said in a statement that he and the other workers in the Washington State Patrol department would miss everyone who has chosen to separate from the department. “I extend a hearty thanks to those who are leaving the agency. I truly wish that you were staying with us. You have my utmost appreciation for the hard and successful work that you have provided during your valued WSP careers. You will forever have our respect for your courage and your commitment in all you have done on behalf of the agency,” said Batiste.
Return to Top	

HEADLINE	**11/03 Candidates of color make election history**
SOURCE	**https://www.npr.org/2021/11/03/1051811110/election-night-2021-results-michelle-wu-eric-adams-ed-gainey-mayor**
GIST	People of color made history on election night in 2021, bringing diversity to leadership roles in some of America's biggest cities, and in some states as well. Boston, New York, Pittsburgh and Dearborn, Mich., were among the places that a majority of voters embraced minority candidates. Here's a rundown of some of the most high-profile wins — a list that we'll be updating as results continue to come in: **Michelle Wu is the first woman and person of color to be elected Boston's mayor** The city councilor and daughter of Taiwanese immigrants broke Boston's 199-year streak of white, male city leaders. Michelle Wu defeated fellow Democratic City Councilor Annissa Essaibi George, a self-described first-generation Arab-Polish American. As NPR's Vanessa Romo reports, "For many, the race came down to competing visions of the future with Essaibi George's version cast as more of the old guard and Wu's perceived as new-school Boston." Here are some of Wu's priorities. **Pittsburgh elects Ed Gainey, the city's first Black mayor ever** Pittsburgh native Ed Gainey, pictured during a visit to his former 4th-grade classroom, is the winner of the city's mayoral race. The western Pennsylvania metropolis, which is 23% Black, largely favored the Democrat Ed Gainey over Republican challenger Tony Moreno. Gainey was born and raised by a single mother in Pittsburgh, where he lived in public housing and later found a career in politics. "We know how people have talked about Pittsburgh, how siloed it is, how segregated it is," Gainey told supporters on Tuesday, according to member station WESA. "But today, you changed that." **Eric Adams becomes the second Black man to lead New York City** New Yorkers chose Democrat Eric Adams, a former police department captain, as the city's second Black mayor. It was lopsided victory for Adams, a former state senator who is currently the Brooklyn borough president. "I am you," he told supporters Tuesday night, according to the Gothamist website. "For a young man from south Jamaica Queens that grew up with all the challenges that New Yorkers face, it is not just a victory over adversity, it is a vindication of faith."

Adams ran on a promise to improve public safety and fight gun violence and to boost the efficiency of the city's police force. More on the race here.

Cincinnati elects Aftab Pureval as its first Asian American mayor
The 39-year-old Democrat started his political career six years ago as an outsider, member station WVXU reports, and last night, he defeated 82-year-old opponent David Mann, "a longtime pillar of Cincinnati City Hall."

The Tibetan-Indian son of immigrants, Aftab Pureval, earned his law degree and worked for Procter & Gamble before running successfully for Hamilton County Clerk of Courts in 2016.

He is the fourth person to be elected under the direct election of the mayor system, in a race that saw remarkably low turnout at 24%. WVXU has more on Pureval here.

Winsome Sears will be the first Black woman to be Virginia's lieutenant governor
Winsome Sears takes the stage on election night. The Republican will become Virginia's next lieutenant governor, reaching new heights for Black women in the state.

It's the highest office a woman of color has won in Virginia's history. Winsome Sears, a Republican, won a race that highlighted diversity: her Democratic opponent, Hala Ayala, comes from a family with Salvadoran, Irish, Lebanese and North African heritage.

"Just 10 Black women in the U.S. have ever held statewide office," member station WAMU reports. "What you are looking at is the American dream," Sears, a pro-Trump former Marine, said, according to WAMU. "I didn't run to make history. I ran to leave it better than I found it ... Help is on the way."

Abdullah Hammoud becomes the first Arab-American and Muslim mayor of Dearborn, Mich.
The Detroit suburb boasts one of the largest Arab communities in the U.S., but that had never been reflected in the city's highest office. Abdullah Hammoud, the son of Lebanese immigrants, dedicated his victory speech Tuesday night to "any young girls or boys who have been ridiculed for their faith or ethnicity." The Democratic state representative defeated his opponent, longtime Michigan politician Gary Woronchak.

Tyrone Garner will be the first Black mayor of Kansas City, Kan.
In his first political race, Tyrone Garner unseated one-term incumbent David Alvey in the race to lead Kansas City, Kan., and Wyandotte County — which have a unified government.

Garner is a former high-ranking police officer. He retired as deputy chief in June 2019, according to member station KCUR. His campaign focused not on getting tough on crime but on improving economic equity and public services, particularly for people in neglected neighborhoods. "I am a forward thinker that wants to be a unifying force to facilitate opportunity, equity and hope," he told KCUR.

Alvin Bragg is Manhattan's new district attorney, the first Black person to hold the job
A native of Harlem, Alvin Bragg was most recently the chief deputy attorney general of New York State. He'll lead an office that's currently pursuing an investigation into former President Donald Trump's business practices. Former Manhattan District Attorney Cyrus Vance Jr. announced earlier this year that he would not seek a fourth term.

Bruce Harrell seizes a big lead in Seattle's mayoral race
Bruce Harrell would be the first Asian American and the second Black person to lead Seattle. All of the city's votes are not yet counted, but Harrell has 65% of the tally as of early Wednesday morning, compared with 35% for Lorena González, who would become the city's first Latina mayor if she manages to stage a comeback.

	Harrell is a moderate who took González, a progressive, to task over her support for defunding the police. "I would say to the abolitionists and the defunders that we need to drive outcomes and invest in outcomes that we want," he said, according to member station KUOW. "We want culturally competent, de-escalating officers who take their oath of office in such a way that they will protect all communities." It will be days before Seattle's vote is final, in part because ballots can still be mailed on Election Day. In recent years, no candidate has surmounted a 30% early deficit, The Seattle Times says. KUOW says, "Seattle's Election Night reflected a regional and national trend, of liberals getting trounced."
Return to Top	

HEADLINE	**11/03 Seattle mayor: death threats, extremism**
SOURCE	**https://www.king5.com/article/news/local/seattle/death-threats-extremism-linked-to-seattle-mayor-durkans-decision-not-to-run-for-re-election/281-fe0bf209-ad0a-4bdd-a521-c93e7ca11ce7**
GIST	SEATTLE — Jenny Durkan will end her time as mayor of Seattle after one term, but that wasn't always her plan. Durkan filed for re-election in early 2020, before the pandemic began and demands to defund the police increased. Those factors are just the beginning of what led to her decision to pull her re-election bid. Durkan was seen as a stabilizing force when she was elected in 2017, fresh off the Seattle City Hall scandal that led to the abrupt resignation of Ed Murray. Durkan was the first woman to be elected Seattle mayor since Bertha Knight Landes in 1926, bringing credibility and a resume that included being the first openly gay U.S. Attorney in history. A week into the job, she finalized a Memorandum of Understanding for what would become Climate Pledge Arena. A day later, the National Hockey League told the city to apply for a new franchise. But the COVID-19 pandemic altered the course of the civic discourse and financial stability. Durkan faced criticism, even from her staunchest allies, for the Seattle Police Department's (SPD) handling of protests on Capitol Hill and negotiations over funding. There was a recall effort and vocal civic groups, some of which were her former supporters, calling for her resignation. Councilmember Kshama Sawant went so far as to lead a march to Durkan's home - her address was hidden by state statute due to her prior career as a U.S. attorney. Durkan's home was vandalized. That single act may have changed her life, especially as there were death threats made not only to her but to her entire family. Before the march, Durkan said she and her family could take comfort knowing that the people who threatened her didn't know where she lived. That all changed when people were led to her house. Reflecting on the unsolved murder of U.S. Prosecuting Attorney Thomas Wales in his Seattle home, Durkan said the fear for her and her family's safety is based on "too much experience, in reality, to know that I got to take it very seriously." The marches to her home continued, as did the death threats and malicious emails. An email from October reads: *"Wishing you and your freak show 'family' nothing but the worst. praying they are all assaulted by the hordes of vagrants you have unleashed on the street."* Durkan said there were times when her son couldn't come home because it wasn't safe, "and we made a decision to remove him from the house."

	At least a dozen death threats have been sent to SPD and the FBI. Two arrests have been made and a restraining order has been issued. Durkan said the threats keep coming. "There's this normalization of really dehumanizing people, and I think that's really a dangerous thing for us," Durkan said. She partially blames the growing extremism seen in politics for her circumstance. "We can't continue and survive as a democracy if that is what happens because good people won't want to serve," she said. The city council has done nothing in regard to the mayor's privacy, she said. She said there should be clear lines, and people need to know "some things just aren't OK." "It's not OK to go to someone's house and spray paint graffiti or to have death threats, and everybody should denounce it," she said. Mayor Durkan said she is still afraid. "I am," she said. "I take the threats to my security seriously, and I fear for my family. You know, as a mom, you want to make sure they're all right and they're protected." The death threats and issues of personal safety factored into Durkan's decision not to run for re-election. However, she's also stepping away from city politics because she is a polarizing figure, and it was time for Seattle to turn the page, she said. Durkan is looking forward to taking a break and focusing on what's most important: family.
Return to Top	

HEADLINE	**11/03 CSIS: Covid most disruptive event post-9/11**
SOURCE	**https://globalnews.ca/news/8347361/covid-19-canadian-intelligence-csis-deputy-director/**
GIST	The COVID-19 pandemic has been arguably “the most disruptive event” since 9/11 for Canadian national security agencies, according to one of the country’s top intelligence officials. Tricia Geddes, a deputy director with the Canadian Security Intelligence Service, said Wednesday the pandemic has both accelerated particular national security threats and made the work of Canadian intelligence agencies more complicated. Geddes said CSIS “saw new threat vectors emerging immediately” at the start of the pandemic: domestic extremists harnessing COVID-19 conspiracy theories for recruitment, an increase in cyber espionage targeting Canadian research and development, and locked-down Canadians conducting sensitive corporate work from unsecured home computers. At the same time, the national security community was dealing with pandemic complications to their work — everything from challenges with meeting sensitive sources in locked-down countries to employees working from home without access to classified material. Geddes suggested that combination has provoked the Canadian intelligence community to think collectively on how to adapt to the new environment. “This has been the most disruptive event probably since 9/11, arguably, for us to have to deal with. And I think it’s time for a proper reflection,” Geddes told a panel hosted by the Canadian Association for Security and Intelligence Studies.

	"It makes sense that we look collectively at how do we build the right systems. There's an opportunity here for us to look at this in a collective way … in some of the bigger investments that we would need to make." That the pandemic has introduced new threats and accelerated existing ones is not a surprise. Canada and allied intelligence agencies have called out Russia for targeting COVID-19 research, warned about the risks of more and more workers dealing with sensitive information while working remotely, and warned about hostile states increasingly turning to economic espionage. But Geddes said Wednesday that CSIS expects these threats to persist even as Canada slowly recovers from the COVID-19 pandemic. "Some hostile state actors were attempting to leverage all elements of state power, including through the use of aggressive and offensive intelligence operations targeting Canadian life sciences research," Geddes said. "While not new, this trend accelerated during the pandemic, and we believe it will continue to be a significant challenge as states emerge from an event that significantly challenges national economies." Geddes' statement is in keeping with Canadian intelligence's increasing focus on economic espionage and theft of intellectual property, including research and development conducted at Canadian universities. But documents obtained by Global News suggest that more traditional forums of national security threats — including domestic extremism — have adapted to the new pandemic reality as well. A June 2020 report from the Integrated Terrorism Assessment Centre, a multi-agency organization tasked with assessing terrorist threats to Canada, suggested "ideologically motivated violent extremists" have "exploited the COVID-19 pandemic through online propaganda to promote their ideologies." A follow-up memo from November 2020, released under access to information law, reported "the increased popularity of pandemic conspiracy theories in Canada, especially in Quebec, are a growing concern that online threats and disinformation could incite extremist violence against politicians and public health officials." Anti-lockdown protesters recently coordinated protests outside Ontario Education Minister Stephen Lecce's house and constituency office. Mobs of anti-vaxxers and COVID deniers shadowed Prime Minister Justin Trudeau during the recent election. And over the weekend, COVID-19 protesters hung a noose outside Alberta MLA Tracy Allard's home, with the words "Hang em all" written across the gallows. Geddes said that CSIS is "aware" that hostile state actors are amplifying COVID disinformation to "exacerbate social and political tensions created by the pandemic." "Those holding these extremist views often attempt to create an online culture of fear, hatred and mistrust by exploiting real or imagined concerns when addressing an online audience," Geddes said. "Major global issues such as the pandemic can, and we did see them, augment extremist efforts to move their message from the fringes of society to the mainstream."
Return to Top	

HEADLINE	**11/03 Logistics woes: truck driver shortage**
SOURCE	**https://www.wsj.com/articles/truck-driver-shortage-supply-chain-issues-logistics-11635950481?mod=hp_lead_pos10**

GIST	Truck driver Chris Wagner pulled his big rig into a grain processing plant in Sidney, Ohio, on a recent afternoon to pick up a load bound for the Chicago suburbs. He'd lost his scheduled place in line because of delays at an earlier delivery, so it was 10:45 p.m. before the plant was ready to load his trailer. By then, the clock had run out on his federally mandated 14-hour workday, so Mr. Wagner couldn't pull up to the dock. He slept that night in his truck on the plant's lot and left empty-handed the following morning, unable to reschedule the pickup. "I sat overnight and still never got loaded," said Mr. Wagner, a 53-year-old retired Marine from Lena, Ill., who drives for Quality Transport Co., a small trucking operator based in nearby Freeport. A critical, often-overlooked link in the supply chain is emerging as a stubborn choke point in the freight-backlog mess: trucking. Trucks haul more than 70% of domestic cargo shipments. Yet many fleets say they can't hire enough drivers to meet booming consumer demand as the U.S. economy emerges from the pandemic. The freight backup has intensified longstanding strains in the industry over hours, pay, working conditions and retention. The surge of goods has created logjams at loading docks and port terminals, gobbling up scarce trucking capacity and making drivers' jobs even harder. Factories and warehouses are also short of staff to load and receive goods. Meanwhile, the broader labor shortage has left openings for other blue-collar jobs that compete with trucking, including in local delivery operations, construction and manufacturing. The shortfalls are pushing up transportation costs and delaying deliveries for retailers and manufacturers already coping with disruptions ahead of the holiday peak. The American Trucking Associations, one of the largest trade bodies, estimates the industry is some 80,000 drivers short of the workers needed to keep goods moving freely this year—up from an estimated shortage of 61,500 drivers before the pandemic. New trucks, trailers and other equipment are in short supply, further limiting the movement of cargo. Trucking payrolls have rebounded from early pandemic lows when efforts to stop the spread of Covid-19 shut down much of the economy. The sector added 74,500 jobs between April 2020 and September 2021, according to seasonally-adjusted Labor Department data, though overall employment in trucking remained 1.3% lower than pre-pandemic levels in September 2019. To help draw more drivers, fleets of all sizes are raising wages and dangling bonuses. The American Trucking Associations is backing proposed legislation to test letting people as young as 18 drive big rigs interstate, a job now limited to drivers 21 and older. Close to a third of drivers now on the road are over age 55, and women make up only 7% of all truckers, the group said. Median annual pay for heavy-truck and tractor-trailer drivers last year was $47,130, according to the Bureau of Labor Statistics, and has increased by about 3% to 4% annually since 2016. Some operators say the biggest problem isn't a shortage of drivers, but a lack of efficiency in a model that hasn't changed much in several decades. Many drivers are paid by the mile, and typically don't get paid for the first two hours spent waiting to load or unload cargo. Even after that window, drivers often don't routinely seek compensation from carriers or freight brokers for that time because they seldom get it, according to a 2020 survey by the Owner-Operator Independent Drivers Association. Any pay for time spent waiting is generally less than what drivers would make when their wheels are rolling.

"The economic dysfunction of trucking is there's no value placed on a driver's time," said Todd Spencer, president of the association, which represents drivers that own or operate individual heavy-duty trucks and small truck fleets.

Now, truckers who used to wait a few hours to pick up or unload cargo sometimes sit as long as 12 hours, said Daniel Faircloth, chief executive of Surge Transportation Group LLC, a Dallas-based carrier with 75 trucks.

To address that, Mr. Faircloth raised the rates he charges his shipping customers and offered to pay his drivers a straight salary of $1,650 a week. "Inefficiency in the entire industry gets under drivers' skin," he said. "You help us get more efficient, and that helps drive rates down."

In September, the average cost to hire a big rig on the "spot market," where companies book last-minute transportation, was $2.49 per mile excluding fuel surcharges, up 14% from the same month in 2020, according to online freight marketplace DAT Solutions LLC. It's the highest monthly average since DAT began reporting that data in 2010. The average price for the long-term contract rates shippers negotiate with trucking companies jumped 23%, to $2.49 per mile, also a new high.

Sadaya Morris, a 28-year-old driver from Plainfield, N.J., used to run loads as an independent contractor for a port trucking company. She started her own business under the name Pink Transportation LLC in September 2020 and can now bid for freight herself, a move she says will improve her earnings.

Ms. Morris said drivers often sit for hours waiting to pick up cargo from the Port of New York and New Jersey, only to get held up again when dropping off freight with customers.

"It's the operations that are the issue," said Ms. Morris, who belongs to a trucker group called PAR18 that is pushing to ensure port drivers get paid for their time. "We're obligated to wait there for two hours for free."

In California, where cargo is piling up at the bottlenecked ports of Los Angeles and Long Beach, recruiting additional drivers has been an uphill battle, said Lisa Wan, director of operations for RoadEx CY Inc., a Carson, Calif.-based operator that hauls cargo from ports to local yards and distribution facilities.

The surge of freight has left port truckers who make those short runs tired and burned out, she said. As of September, import volumes at the ports of Los Angeles and Long Beach were 25% higher year-to-date compared with the same period in 2020.

Some port truckers who make those runs have switched to become long-haul drivers, who move freight over a distance of 250 miles or more, as rates to move goods out of state have skyrocketed, Ms. Wan said. Other drivers have turned to local delivery work, which doesn't typically involve overnights on the road, or left the industry altogether, opting for jobs with more predictable hours.

Jesse Milligan of West Lafayette, Ohio, is a third-generation trucker who started driving in 2009, after he got laid off from a steel mill. He hauled lumber, chemicals and military vehicles all over the country with his father, who owned his own truck, then bought the vehicle and went into business for himself.

He took a local job in September last year delivering and installing propane systems to spend more time with family. The pay is on the lower end of what he used to make, at around $50,000 a year, he said, but he gets home every night. With long-haul trucking, "you need to be on the road a couple of weeks at the time," said Mr. Milligan, 37. "It's just too hard with kids to plan anything."

Carriers on average will end up paying drivers about 8% more this year, according to the National Transportation Institute, a research group that benchmarks trucking industry wages. Pay varies widely, with some truckers earning $45,000 a year while drivers for private fleets that move goods for manufacturers or retailers can make well over $100,000 a year, NTI Chief Executive Leah Shaver said.

The ATA said pay increases mean some drivers will choose to work less at higher rates, further denting capacity.

“If they can make in two or three days what would normally take them a week, they’ll go home,” said Jerry Gioia, an owner-operator with a four-truck fleet based in Hayden, Colo.

Big trucking companies warn that the transportation problems, and higher rates, could extend into next year due to labor and equipment shortages and the backlog of freight.

“Really, it’s all about drivers,” Eric Fuller, chief executive of US Xpress Enterprises Inc., a large Chattanooga, Tenn.-based trucking company, told investors in an Oct. 21 earnings call. “We can’t find enough people that want to do the job.”

Many long-haul drivers say that although they like the freedom of driving on the open road, truckers often quit because of low pay and poor treatment by both employers and customers.

Tyler Foster, 53, a long-haul driver from Green River, Wyo., said that some big trucking companies treat workers like they’re expendable. “They just run them hard, they get very little pay and they leave after three to six months,” he said.

Some customers aren’t much better, Mr. Foster and other truckers said, and make drivers wait hours for freight under conditions that have gotten worse since businesses added restrictions aimed at curbing the spread of Covid.

“The shippers, they treat us like criminals, basically. Don’t use the bathroom, don’t get out of your truck,” Mr. Foster said. “The port-a-potty’s in the yard, but it’s 25 degrees out.”

Some companies are working with carriers to address those problems by streamlining the way they receive freight and keeping facilities like bathrooms and waiting rooms open to drivers, said Gail Rutkowski, executive director of the National Shippers Strategic Transportation Council, which represents transportation professionals at businesses that ship and receive goods, including retailers, manufacturers and distributors.

Drivers and fleet owners also say that government regulations can be intrusive or cut into driver earnings, pushing some to leave. Those include rules intended to reduce fatigue by electronically tracking drivers’ time behind the wheel, or to curb pollution near the ports of Los Angeles and Long Beach by phasing out the use of older trucks.

Some truckers say that a number of California drivers have either left the state or taken other jobs because of a 2020 law that seeks to require companies there to classify independent contractors as employees. The California Trucking Association has said that the measure would essentially ban a common industry practice and harm independent truckers that haul freight for trucking companies operating in California. The association has asked the U.S. Supreme Court to review a case challenging its application to trucking.

Steve Viscelli, a sociologist at the University of Pennsylvania who studies the industry, said that trucking’s hiring challenges largely stem from a labor model that churns through inexperienced drivers.

“There is absolutely not a shortage of people licensed and trained to do that job,” Mr. Viscelli said. “The industry has burned so many of them that they left.”

In California, more than 468,000 people hold Class A commercial driver’s licenses, allowing them to operate vehicles including heavy-duty trucks and tractor-trailers, according to June data from the state’s department of motor vehicles. Mr. Viscelli estimated that less than half that number are working in jobs in the state requiring that license, and said nationally there are millions more people certified as commercial drivers than are currently working as truckers.

	"If we wanted to add capacity quickly," he said, "the big question is how to get people to come back?" Reducing on-the-job hardships, such as a lack of parking and extended wait times, would help make the job more rewarding for drivers, said David Heller, vice president of government affairs for the Truckload Carriers Association. "If you lower those waiting times to the minimum amount that you needed to do, all of the current existing drivers could haul more freight, which essentially means you increase effective capacity without adding one truck," ATA Chief Economist Bob Costello said. Jim Orr, a 65-year-old independent trucker from Chandler, Okla., doesn't take loads from customers who keep him waiting. He rarely works more than 500 miles from his home, and doesn't have much sympathy for businesses that complain about high trucking rates. That's capitalism, Mr. Orr said. "I'm sure they weren't concerned two years ago when we were lucky to be getting half of what we are now. It's the market…feast or famine."
Return to Top	

HEADLINE	**11/03 Vaccine rollout for children begins**
SOURCE	**https://mynorthwest.com/3217990/vaccine-rollout-children-washington-state/**
GIST	Children between the ages of 5 and 11 in Washington state could start receiving the COVID-19 vaccine within the next few weeks, following its approval by the Western States Scientific Safety Review Workgroup. That came after Pfizer's two-dose vaccine cleared two final hurdles at the federal level Tuesday, having now received approval from advisers at the Centers for Disease Control and Prevention and CDC Director Dr. Rochelle Walensky. "Parents can breathe a sigh of relief that their younger kids can now be vaccinated against the deadly COVID-19 virus," Gov. Jay Inslee said in a news release. "This gets us a step closer to having the entire population of Washington eligible for the vaccine. And a step closer to finding our way out of this pandemic." With final approvals out of the way, rolling the vaccine out to children will still likely be a gradual process. Seattle-King County Public Health noted Wednesday that its distribution sites "do not yet have appointments available for this age group," and that shipments from the CDC may not arrive for some providers until next week. That said, Harborview Medical Center reportedly received 5,700 doses for children Tuesday. Parents can call 844-520-8700 to get their children on the waiting list. Once a child's turn comes up, UW Medicine will reach out to set up an appointment time. Moving forward, UW Medicine plans to offer the vaccine to children in the 5-11 age group at all of its hospitals and neighborhood clinics once more doses are available. City of Seattle clinics at Amazon downtown and in West Seattle will also begin administering doses to children starting this weekend by appointment only at this link. "With nearly 183,000 five to eleven year olds in King County now eligible for the COVID-19 vaccine, doses at City of Seattle vaccination sites will be extremely limited for the next two weeks," Mayor Jenny Durkan's office said. Local health officials have stressed the relative safety of the vaccine for children, particularly when weighed against the negative effects of COVID-19.

	"We're still learning about the impact of long COVID on children, and we know children can spread COVID-19 to others, including adults who may be vulnerable to severe outcomes," King County Health Officer Dr. Jeff Duchin said. "For these reasons, along with the strong safety record of the vaccine in older children and adults, we look forward to ensuring access to the pediatric vaccine as soon as possible."
Return to Top	

HEADLINE	**11/03 Alaska: ignore federal vaccine mandates**
SOURCE	**https://arstechnica.com/science/2021/11/despite-sky-high-case-rates-alaska-governor-wages-war-on-vaccine-mandates/**
GIST	Though the state of Alaska currently has the highest rate of COVID-19 cases in the country, Governor Mike Dunleavy is focusing on fighting federal vaccine mandates. Dunleavy signed an administrative order Tuesday that prohibits all state agencies from participating in or assisting with federal vaccine mandates for employers. The order also tasks the state's attorney general with reviewing all federal vaccine mandates and looking for ways to challenge them in court. Last week, Alaska also joined nine other states in filing a lawsuit challenging the Biden administration's vaccine mandate for federal contractors. And in an opinion piece published Monday on a far-right political website, Dunleavy vowed that Alaska would also take legal action against an upcoming rule by the Occupational Health and Safety Administration to compel companies with 100 or more employees to require vaccination or regular testing. White House COVID-19 Response Coordinator Jeff Zients said Wednesday that the rule will be coming in a matter of days. Dunleavy argues that the federal mandates and rules are "unconstitutional" and "completely unnecessary" for the state of Alaska, which has only 53 percent of its population vaccinated. The Republican governor claims Alaska has "handled COVID better than nearly every other state in the US." He boasted that the state has never had a mask mandate and ended its emergency declaration before other states. The state also never prevented healthcare providers from offering unproven and potentially harmful treatments for COVID-19, such as ivermectin and hydroxychloroquine, Dunleavy proudly noted. And, so far, Alaska has the fourth-lowest COVID-19 death rate among states. Mandating success But Alaska also has the second-highest COVID-19 case rate overall in the country, with 19,000 cases per 100,000 people since the pandemic began, according to data tracking by the New York Times. Alaska is second only to North Dakota, with 19,584 cases per 100,000 overall in the pandemic. And Alaska currently has the highest daily case rate of any state or jurisdiction in the country, with 82 daily cases per 100,000 people. The state is now reporting a seven-day average of around 600 new cases per day, down from a peak of over 1,300 at the end of September. Last month, amid the peak of the state's delta wave, Alaska officials activated emergency crisis protocols in 20 medical facilities, allowing healthcare providers to ration care amid a crush of COVID-19 patients. Dunleavy, who is up for reelection next year, is facing criticism from political opponents over his handling of the pandemic and his recent efforts to fight vaccine mandates. Democratic gubernatorial candidate Les Gara told Anchorage Daily News that Dunleavy "should be working overtime to find ways to convince people that vaccines are safe, save lives, and are one of the only ways out of this pandemic." Though vaccine mandates have faced opposition nationwide, that opposition is small—usually just a sliver of workers and communities—and the mandates have proven remarkably effective, again and again. Just on Tuesday, New York City Mayor Bill de Blasio announced that 92 percent of the city's 378,000 employees were vaccinated, with thousands getting shots as the deadline neared. Though there were concerns that more than 22,000 city workers would buck the requirement, causing mass disruption in city services, only 9,000—less than 6 percent of workers—were placed on unpaid leave this week. Mayor de Blasio said no disruptions were expected.
Return to Top	

HEADLINE	**11/03 DOH: 733,535 cases, 8727 deaths**
SOURCE	**https://www.thenewstribune.com/news/coronavirus/article255528836.html**
GIST	The Washington state Department of Health reported 1,691 new COVID-19 cases and 31 deaths Wednesday. As of Wednesday, statewide totals from the illness caused by the coronavirus are 733,535 and 8,727 deaths. The case total includes 86,793 infections listed as probable. Death data is considered complete only through Oct. 17. DOH revises previous case and death counts daily.
Return to Top	

HEADLINE	**11/03 Ex-SPD chief Best on short list lead NYPD?**
SOURCE	**https://www.seattletimes.com/seattle-news/former-seattle-police-chief-carmen-best-reportedly-on-short-list-to-lead-nypd/**
GIST	Former Police Chief Carmen Best, who oversaw the Seattle Police Department during the city's tumultuous 2020 racial-justice protests, is reportedly a finalist to lead the New York Police Department. Citing multiple unnamed sources, the New York Post reported Wednesday that Best is among three candidates considered "front-runners" on New York Mayor-Elect Eric Adams' short list for police chief consisting of six to eight women. The New York Times also reported Wednesday, based on an unnamed source, that Best is among "at least two Black women" under Adams' consideration for the NYPD commissioner's job. Best, during an interview with The Seattle Times on Wednesday about her new book, "Black in Blue: Lessons on Leadership, Breaking Barriers, and Racial Reconciliation," brought up the Post report from the start of the discussion, saying she didn't want to comment or talk about it. When asked later in the interview if she'd ever consider being a police chief again, she responded: "When it comes to the future, I'm not ruling anything out." Others cited in the Post's report as potential candidates to lead the nation's largest police department include Philadelphia police Chief Danielle Outlaw and former Newark, New Jersey, Police Chief Ivonne Roman. The Times report referenced NYPD's current patrol chief, Juanita Holmes, as another potential candidate. With more than 36,000 officers and 19,000 civilian employees, the New York City police agency dwarfs the roughly 1,200-officer Seattle department that Best headed for two years before abruptly leaving amid the fallout and budget cuts of the 2020 demonstrations. After initially being passed over for the top job in Seattle, Best, then interim chief, was named the permanent chief in 2018 by Mayor Jenny Durkan after a community uproar. She led the department amid last year's weeks-long racial justice and police reform protests following the murder of George Floyd by Minneapolis police. Best, 56, who became a frequent guest on national cable TV talk shows during the unrest, announced her abrupt retirement from the chief's job after City Council proposals to slash the department's budget. In her book, which was released last week, Best blames the council's treatment of her and its pursuit of 50 percent police funding cuts as the reason for her departure. Parts of the book about what happened during the events of 2020 have been disputed by council members and others critical of the department's use of tear gas and other heavy-handed tactics under Best's command that drew public outrage, lawsuits and a federal judge's contempt order against SPD. In June, former City Councilmember and mayoral candidate Bruce Harrell, who now appears headed to victory in Seattle's race for mayor, said in an interview with The Seattle Times he considered Best a "model" police chief he still seeks advice from about public-safety issues. Harrell likely will preside over

	the selection of the city's next chief of the Seattle department, which faces a staffing crisis and remains under federal oversight under a consent decree. Asked in June if he would consider bringing Best back, Harrell said: "I won't exclude that at all." Best, in her interview Wednesday, said she has "a huge amount of respect" for Harrell, but added: "I'm not considering being the chief in Seattle again."
Return to Top	

HEADLINE	**11/03 Set clocks back Sunday**
SOURCE	**https://www.seattletimes.com/seattle-news/why-we-need-to-set-clocks-back-sunday-even-though-washington-voted-to-ditch-the-switch-in-2019/**
GIST	Washington state Rep. Marcus Riccelli isn't quite ready to give up on the popular bipartisan movement to adopt permanent daylight saving time and do away with the biannual clock switch. But we still have to set our clock back one hour on Sunday, Nov. 7. Two years ago, Washington legislators voted to adopt permanent daylight saving time. Similar pieces of legislation were sweeping through the U.S. with 16 other states, including California, Idaho and Oregon passing similar laws, resolutions or voter initiatives. The premier of British Columbia vowed to join the West Coast if Congress approved the change. Changes seemed imminent then, but Congress has not acted on the Sunshine Protection Act, sponsored by U.S. Sen. Patty Murray of Washington and Sen. Marco Rubio of Florida, that would amend the Uniform Time Act of 1966 and allow states to adopt permanent daylight saving time. While states can move to permanent standard time without federal approval, congressional action is required to stay on daylight saving time. Granted, a lot has happened in the last two years, Riccelli said this week, but that shouldn't mean the end of the popular proposal. "People have decided they want this and they are tired of seeing Congress as a broken clock," he said. "Congress needs wins, things that everybody can get behind and they need to take a stronger look at this." A poll by The Associated Press and NORC Center for Public Affairs Research showed that 71% of Americans don't want to keep moving the clock in spring and fall, though they are divided on whether they prefer standard or daylight saving time. In areas of the country at lower latitude, the difference is not so stark, but it's keenly felt in the Seattle area. On Seattle's shortest winter day, the sun rises at about 8 a.m. and sets around 4:20 p.m. If we were to adopt permanent daylight time in the winter, as proposed, the sun would rise at about 9 a.m. and set around 5:20 p.m. Steve Calandrillo, a professor at the University of Washington School of Law who has testified before legislators and written extensively on the benefits of year-round daylight time, has said that numerous studies show permanent daylight time has distinct advantages. Proponents of the measure say it would save hundreds of lives each year because darkness in the late afternoon and evening — when most people are awake and moving around — is more dangerous than the dark of morning, when a significant portion of the population is asleep. It could lead to an estimated 20% reduction in crime because, Calandrillo says, it removes one hour from the "preferred workday" of criminals, who like to act in darkness and "are notoriously late risers."

Among the most common opposition comes from people with concerns about children standing at bus stops in the dark.

However, local experts in depression and sleep science say there are more significant reasons to either embrace the twice-yearly clock change or to adopt permanent standard time instead of daylight saving time.

Both options are more in line with our natural circadian rhythms, which are synced with morning light and are critical for well being, Dr. David Avery, a professor emeritus in the UW School of Medicine's Department of Psychiatry and an expert in seasonal affective disorder (SAD) has said.

Moving our clocks forward into "daylight time," essentially losing an hour of morning light and tacking it onto the evening, is devastating for people with seasonal depression, he said.

"I think people are so focused on the idea of having more light in the evening that they don't think about how this is, in effect, morning light reduction time," said Avery.

In 2011, Russia rejected the notion of changing the clocks and moved to stay permanently on daylight saving, or summer, time.

The move was determined to be a failure after three years, he said, when studies showed a decrease in academic performance among high-school students and higher rates of winter depression, mortality and cancer.

"I just think this is a massive experiment and that there are going to be some unexpected consequences from this," he said. "Even night owls will hate it."

Russian President Dmitry Medvedev, told The Guardian that Russians were fed up with the time changes because they caused "stress and illnesses" and "upset the human biorhythm."

"It's irritating, people wake up early and don't know what to do with themselves for the spare hour," he said. "And that's not to mention the unhappy cows and other animals that don't understand the clocks changing and don't understand why the milkmaids come to them at a different time."

The change in Russia was initially popular, but it became widely disliked in a short time and was abolished in 2014 with the lower house of parliament voting 442 to 1 to return to standard time and stay there.

Officials said permanent summer time created stress and health problems, especially for people in northern Russia. They cited medical reports of increased morning road accidents in 2012 compared to previous years, blaming them firmly on the 2011 time change, the BBC reported.

Avery said switching the clock back and forth is not ideal, but it's the best option among the choices: permanent standard time, permanent daylight time or our current method of springing forward and falling back.

Riccelli said he wants the conversation to begin in Washington state next year and he's willing to have the conversation include a move to permanent standard time, though he and most of the voters he heard from, prefer daylight saving time.

"Anything we can do to ditch the switch and never go back makes sense."

Return to Top

HEADLINE	**11/03 Pentagon: China 1,000 nuke warheads 2030**
SOURCE	**https://www.nytimes.com/2021/11/03/us/politics/china-military-nuclear.html**

GIST

WASHINGTON — China is continuing to strengthen its strategic nuclear arsenal and could have 1,000 nuclear warheads by 2030, according to a new Defense Department report released Wednesday.

The Pentagon's annual report to Congress on China's military might estimates that China could have 700 deliverable nuclear warheads by 2027 and 1,000 three years later. In addition, it warns that China has "possibly already established a nascent nuclear triad with the development of a nuclear capable air-launched ballistic missile and improvement of its ground and sea-based nuclear capabilities."

Even with the accelerated nuclear expansion, Beijing is still behind the United States, with its nuclear stockpile of 5,550 warheads, and Russia, which has 6,255, according to the Stockholm International Peace Research Institute, an independent organization. China has about 350 nuclear warheads, the organization said.

But Beijing has refused to join arms control talks, arguing that its nuclear arsenal is far smaller than those of the world's two major nuclear powers. At the same time, it has pursued a broad military modernization program that has raised questions about its intentions.

The American military's most senior officer said on Wednesday that he views China as the "No. 1" nation-state military challenger to the United States. The comments, by Gen. Mark A. Milley, the chairman of the Joint Chiefs of Staff, during a discussion moderated by NBC's Lester Holt at the Aspen Security Forum, came a week after he characterized China's recent launch of a hypersonic weapon designed to evade American defenses as a near "Sputnik" moment, in an allusion to the Soviet launch of a satellite in 1957, which spooked the American public and helped spur the nuclear arms race during the Cold War.

China, General Milley said on Wednesday, is "clearly challenging us regionally, and their aspiration is to challenge us globally." He added that "they have a China dream, and they want to challenge the so-called liberal rules-based order."

Asked if the United States could "match" China's hypersonic capability, General Milley declined to answer. But he said later that "if we in the United States don't do a fundamental change ourselves, then we will be on the wrong side of a conflict."

General Milley said the United States "absolutely" could defend Taiwan from an attack by China if — and that part is a big if — political leaders decided to do so. Such a decision by any American president would be a huge shift, since the United States for decades has followed a policy of "strategic ambiguity" that leaves open the question of whether the United States would back Taiwan in a military conflict with China. General Milley did not veer from that policy on Wednesday.

He said he did not expect China to take military action against Taiwan in the next 24 months. But when pressed on whether the Pentagon could defend Taiwan, he said that "we absolutely have the capability to do all kinds of things around the world, to include that, if required."

On China's reunification with Taiwan, he added that "the Chinese are clearly and unambiguously building the capability to provide those options to the national leadership if they choose at some point in the future." China considers Taiwan a breakaway province.

China's most recent defense strategy, released in 2019, said it would keep its "nuclear capabilities at the minimum level required for national security." Beijing has also vowed not to use nuclear weapons first or against any non-nuclear state.

Perhaps surprisingly, the Pentagon report makes little mention of the coronavirus pandemic, which began in China in 2019 and spread globally, killing more than 5 million people so far and infecting millions more.

The Pentagon report also backs General Milley's account of his phone calls with his Chinese counterpart in late 2020 to reassure China that the United States under President Donald J. Trump had no intention of attacking.

	According to the report, the calls came at the direction of Mr. Trump's secretary of defense at the time, Mark T. Esper, whom Mr. Trump would later fire.
Return to Top	

HEADLINE	**11/03 China military consistently beats estimates**
SOURCE	**https://www.washingtontimes.com/news/2021/nov/3/chinas-military-consistently-beats-us-estimates/**
GIST	The capabilities of the Chinese military continue to beat U.S. estimates, and neither the Soviet Union at the height of the Cold War nor any other country in recent history has consistently exceeded Pentagon and intelligence community projections to this extent, a top Air Force general said Wednesday. In an exclusive interview with The Washington Times, Lt. Gen. S. Clinton Hinote, the Air Force's deputy chief of staff for strategy, integration and requirements, offered a blunt assessment of how quickly the Chinese armed forces have accelerated key programs such as hypersonic weapons, nuclear arms, and a host of others. Gen. Hinote's sobering take came just hours after a new Pentagon report revealed that the U.S. now expects China to have 1,000 deliverable nuclear warheads by 2030 — beating Defense Department projections offered just last year. "One of the most interesting things about being a China-watcher over maybe the last 10, 15 years has been it's the only country certainly in my memory, and I've had people in the intelligence community tell me that they've never seen a country that consistently accelerates faster than we estimate," he told The Times. "The Soviets didn't do that. Certainly not North Korea or Iran, anything like that. But China has done a good job of taking their economic power … and applying that to acceleration of military capability. And this is why you're seeing things like the hypersonic test" conducted by China last summer and recently confirmed by top Pentagon officials. "I always expect China is going to be pushing the edge of that envelope increasingly forward," he said. Gen. Hinote — who has loudly and repeatedly sounded the alarm about how China is approaching or already at parity with the U.S. by some military metrics — said that the Pentagon is well aware of Beijing's major investments in hypersonic weapons. But he said the specifics of last summer's test did surprise top military leaders. "The way they tested this last one did catch people by surprise. And I think that shows this is a very capable country that is committed to increasing its military power. And it's going to do that. It's going to pursue power," Gen. Hinote said. The frantic pace of China's military expansion has become the defining challenge for Gen. Milley, Gen. Hinote and other leaders across the Pentagon. Defense Secretary Lloyd Austin, for example, calls China the "pacing challenge" for the U.S., with virtually every major initiative inside the Pentagon being measured against the capabilities now being wielded by Beijing and its People's Liberation Army (PLA). In some areas, such as the number of ships in each country's navy, for example, China has already pulled ahead of America — though analysts say that the U.S. Navy's overall capabilities remain superior. But raw numbers and specific vehicles and equipment are just parts of a much bigger, more complex set of problems posed by China and its military ambitions. For U.S. planners, the greatest challenge is developing realistic plans to defend allies halfway around the world from Chinese military aggression. The most pressing example is the potential defense of Taiwan, the island state China regards as a breakaway province. Gen. Hinote said U.S. war game exercises and other planning sessions in recent years have focused intensively on the very daunting problems posed by a Chinese attack on Taiwan. Chinese military capabilities that may be beyond American projections make those problems even more difficult to solve.

	"We have to be able to stop it. We have to be able to defend Taiwan. We have to be able to sink their navy and shoot their aircraft that are coming at and attacking Taiwan," Gen. Hinote said. "And that's really, really hard because it's basically on China's front door step. It's like us trying to invade Cuba and China trying to figure out how to defend it."
Return to Top	

HEADLINE	**11/03 CBO: citizenship path for illegals $500B**
SOURCE	**https://www.washingtontimes.com/news/2021/nov/3/citizenship-path-illegal-immigrants-cost-taxpayers/**
GIST	Offering a path to citizenship to illegal immigrants and opening the doors to more legal immigrants will cost the federal government more than $500 billion over the next few decades, the Congressional Budget Office said Wednesday. The costs would come chiefly to Social Security, Medicare and other social safety net programs that the new, and newly legalized, immigrants would be able to access, the budget analysts said. The nonpartisan budget agency analyzed House Democrats' plan to update the window of eligibility for illegal immigrants to adjust their status to legal immigrants, and to expand availability of green cards, or legal immigrant visas, to more foreign citizens. The total cost of the immigration provisions over the next decade comes to about $140 billion, offset by about $19 billion in new revenue. The two decades after that would be even more expensive for the federal government, costing more than $563 billion in new spending and sapping about $2 billion from revenue. The analysis looked at the costs to the federal government, but did not analyze the impact on the broader U.S. economy. Those who support legalization and expanding future paths for more legal immigration argue that the real benefits come with a larger economy and more taxpayers expanding the government's revenue base. Previous CBO research has indeed confirmed that more workers means a larger GDP, though CBO analysts also say per capita GDP would be lower, because the larger economy is spread over more people. Democrats are trying to shoehorn legalization into President Biden's $1.75 trillion social spending budget package, which deals with climate change, tax credits and prescription drug pricing. The House Democrats' expansive plans envision legal status for illegal immigrant "Dreamers" and others here under special humanitarian protections, as well as "essential" workers. Previous estimates suggest that could cover as many as 8 million people, though the CBO did not release its own figure. The House proposal is unlikely to survive Senate budget rules on what can be included in special "reconciliation" bills that do not need to overcome a minority filibuster. Instead, senators are pondering a more limited legalization that would grant a short-term deportation amnesty to illegal immigrants. That would allow them to obtain work permits, but does not include a clear pathway to citizenship. That plan has not yet been publicly analyzed by the CBO.
Return to Top	

HEADLINE	**11/03 Pentagon details China info war on US**
SOURCE	**https://www.washingtontimes.com/news/2021/nov/3/pentagon-details-china-info-war-us/**
GIST	China is engaged in influence operations targeting U.S. society aimed at building support for the communist nation's policies and strategies, according to the Pentagon's latest annual report on the Chinese military.

"The PRC conducts influence operations, which target cultural institutions, media organizations, business, academic, and policy communities in the United States, other countries, and international institutions, to achieve outcomes favorable to its strategic objectives," the report said.

Little academic research has been done in the United States to track the influence operations, which have been successful in shaping Americans' understanding of China. Many media organizations and think tanks often reflect Chinese government propaganda and messages, such as the theme that China poses no threat to the U.S.

Beijing uses its funding and access to travel in China as means of influencing American institutions to avoid criticizing threatening activities such as human rights violations and China's spread of nuclear arms and equipment around the world.

The ruling Chinese Communist Party (CCP) "seeks to condition domestic, foreign, and multilateral political establishments and public opinion to accept Beijing's narratives and remove obstacles preventing attainment of goals," the 192-page report contends. Beijing's communist leaders believe open democratic societies are more susceptible to its influence operations.

According to the report, the People's Liberation Army is using the "three warfares concept" to guide its activities: psychological warfare, public opinion warfare and legal warfare. All have been in the military's playbook since at least 2003.

The report notes that the PLA is developing advanced "digital influence capabilities" in its information warfare campaigns by incorporating artificial intelligence, which it hopes will improve the quality and deniability of its messaging.

The Chinese military has even created a special service for information and influence campaigns, called the Strategic Support Force. Within the force, the network systems department is in charge of information warfare using cyberwarfare, technical reconnaissance, electronic warfare (EW) and psychological warfare.

"By placing these missions under the same organizational umbrella, the PRC seeks to remedy the operational coordination challenges that hindered information sharing under the PLA's pre-reform organizational structure," the report said.

The network system department is in charge of the three warfares operations.

The information warfare component seeks to "demoralize adversaries [and] influence foreign and domestic public opinion," the report said.

"Psychological warfare uses propaganda, deception, threats and coercion to affect the adversary's decision-making, while also countering adversary psychological operations," according to the report.

Public opinion warfare involves spreading information for public consumption that will guide and influence public opinion and build support from domestic and international audiences. And legal warfare is the exploitation of laws to gain international support, limit political repercussions and sway target audiences.

Increasingly, the Chinese are using digital influence operations as well, including efforts to support China's interpretation of the "one-China policy" regarding Taiwan; to back the economic expansionist development scheme called the Belt and Road Initiative; to gain support for China's takeover of democratic Hong Kong; and to back Chinese disputed territorial claims in the South China Sea and East China Sea.

"PRC influence operations are coordinated at a high level and executed by a range of actors, such as the United Front Work Department, the Propaganda Department and the Ministry of State Security (MSS)," the report said.

The operations often target overseas Chinese or ethnic Chinese living abroad through what the report called "soft-power engagements." Blackmail and coercion to manipulate overseas Chinese also are used, such as threatening ethnic Uyghurs living in the United States with imprisonment of family members in China.

The operations also are used to support the acquisition of American technology, such as the "Thousand Talents Program," which has recruited several U.S. researchers who were paid covertly by China. Some of the more than 200,000 Chinese students in the United States also are ordered to spread the official Chinese government line, such as opposing Tibetan human rights activists and the Dalai Lama.

The main vehicles are Chinese Students and Scholars Associations (CSSA) and Confucius Institutes, which seek to support Chinese policies and lodge protests on college campuses over activities that "fail to comport with Beijing's narrative," the report said.

"The PRC's foreign influence activities are predominantly focused on establishing and maintaining influence with power brokers within foreign governments to promote policies that the PRC views will facilitate its rise, despite Beijing's stated position of not interfering in foreign countries' internal affairs," the report says.

Chinese diplomats also seek to influence well-connected Americans by providing assistance and calling for "win-win cooperation" through trade and diplomacy.

Some nations are fighting back. The European Union, Australia and New Zealand are seeking ways to curb the influence operations.

The report said the PLA has voiced concern that the United States is using the internet and social media to undermine the Chinese Communist Party's hold on power domestically. The PLA, in response, is researching digital influence operations by sending teams to Russia, Israel, Belarus and Germany to study operations there.

The PLA may set up its own Twitter account and other accounts on Western social media. The military also is using covert social media accounts for its political influence operations.

PLA Strategic Support Force personnel "may have conducted a covert social media campaign to support pro-PRC candidates and try to sway the outcome of the 2018 Taiwan election," the report said.

The PLA also is preparing to use "deep fakes" — high-quality doctored videos designed to smear public figures.

"In 2019, PLA personnel also suggested training [artificial intelligence] algorithms to autonomously create content and coordinate influence activity between different fake accounts," the report said.

BEIJING NOW WANTS MILITARY SUPERIORITY OVER U.S.

As part of its drive to develop a world-class military by 2049, China's leaders are seeking to achieve superiority over the United States, according to the Pentagon's latest report on China's military power.

"It is likely that [China] will seek to develop a military by mid-century that is equal to — or in some cases superior to — the U.S. military, and that of any other great power that Beijing views as a threat to its sovereignty, security and development interests," the report said.

	As part of Chinese President Xi Jinping's drive for national rejuvenation, "it is unlikely that the [Chinese Communist Party] would aim for an end state in which China would remain in a position of military inferiority vis-a-vis the United States or any other potential rival," the report states. The report was produced in part by the Defense Intelligence Agency and reverses judgments some 25 years ago in earlier annual reports that said China had few global ambitions and sought mainly to limit its military buildup to forces that could retake Taiwan. The Pentagon now believes China will not settle for less than being the world's most powerful nation. However, the People's Liberation Army is not likely to mirror the U.S. military in terms of capabilities and power. "The PRC will likely seek to develop its 'world-class' military in a manner that it believes best suits the needs of its armed forces to defend and advance the country's interests and how the PLA — guided by the Party — adapts to the changing character of warfare." The report notes that the Chinese military is not a national army like those of other nations. "The PLA is the principal armed wing of the CCP and, as a party-army, does not directly serve the state," the report says. "As a party-army, the PLA is a political actor. As a constituency within the Party, it participates in the PRC's political and governance systems. As the ultimate guarantor of the Party's rule and political and governance systems, the PLA's missions include formal and informal domestic security missions in addition to its national defense missions." Visible differences between the party and PLA leaders are extremely rare, and official propaganda in recent years has emphasized absolute party control over the PLA — despite the fact that the officer corps is almost exclusively made up of Communist Party members.
Return to Top	

HEADLINE	**11/03 Climate summit: phase out coal-fired power**
SOURCE	**https://www.theguardian.com/environment/2021/nov/03/more-than-40-countries-agree-to-phase-out-coal-fired-power**
GIST	More than 40 countries have agreed to phase out their use of coal-fired power, the dirtiest fuel source, in a boost to UK hopes of a deal to "keep 1.5C alive", from the Cop26 climate summit. Major coal-using countries, including Canada, Poland, Ukraine and Vietnam, will phase out their use of coal for electricity generation, with the bigger economies doing so in the 2030s, and smaller economies doing so in the 2040s. However, some of the world's biggest coal-dependent economies, including Australia, China, India and the US were missing from the deal, and experts and campaigners told the Guardian the phase-out deadlines countries signed up to were much too late. The goal of "consigning coal to history" has been a key focus for the UK as host of the Cop26 summit, which aims to put the world on track to limit global heating to 1.5C above pre-industrial levels. Kwasi Kwarteng, the UK's business secretary, said: "Today marks a milestone moment in our global efforts to tackle climate change, as nations from all corners of the world unite in Glasgow to declare that coal has no part to play in our future power generation. Today's ambitious commitments made by our international partners demonstrate that the end of coal is in sight."

Coal use is one of the biggest causes of greenhouse gas emissions, according to the International Energy Agency, and use of the polluting fuel has rebounded after the temporary plunge in emissions caused by last year's lockdowns.

The deal brokered by the UK at Glasgow includes commitments from dozens of developing as well as developed countries to stop using coal, and more than 100 financial institutions and other organisations have also agreed to stop financing coal development.

The deal came as part of a focus on energy for the fifth day of the Cop26 summit, and follows a spate of previous announcements earlier in the week, such as a commitment from scores of countries to halt deforestation. Also on Wednesday:

- More than 20 governments and financial institutions, including the UK, US and Denmark, agreed to phase out overseas finance for all fossil fuels.
- Research showed that the world could be on track to limit global heating to 1.9C, if commitments from India and other countries on greenhouse gas emissions are fulfilled.
- Data seen by the Guardian revealed fossil fuel companies were using the energy charter treaty to sue governments for the losses they incur from national commitments to decarbonise.
- Ireland was told it would need to cull 1.3m animals to meet climate targets.
- The UK chancellor, Rishi Sunak, told the Cop26 conference London would become a global hub for net zero investment.

The suite of announcements on coal is a key pillar of the UK's strategy for Cop26. Leading figures acknowledged to the Guardian before the two-week conference began that the core aim – of getting countries to produce national emissions-cutting plans that would add up to a halving of greenhouse gas emissions by 2030, compared with 2010 levels, which scientists say is needed to stay within 1.5C – would not be fulfilled.

So in order to close the gap between countries' headline carbon-cutting commitments and the 45% reduction in emissions needed, part of the UK's strategy is to focus on major areas of importance to the climate – "cash, coal, cars and trees" in the mantra espoused by Boris Johnson – that will produce key progress in tackling the climate crisis.

Many campaigners welcomed the suite of announcements on coal, which also included a commitment by more than 20 countries – understood to include the US, as well as the UK and Denmark – to stop funding any fossil fuel development overseas by the end of 2022, and divert the estimated $8bn (£5.85bn) a year saved into clean energy investment instead.

Chris Littlecott, social director at the thinktank E3G, said: "This commitment on coal is definitely a big step forward, and would have been unthinkable a year or two ago. It's a real sign of improvement."

But others said the move did not go far enough. Jamie Peters, director of campaigns at Friends of the Earth, said: "The key point in this underwhelming announcement is that coal is basically allowed to continue as normal for years yet. Some people may hear what the prime minister said at the opening of Cop, compare it to this, and wonder why there is such a difference between words and action. "

Expert assessments have found that for the world to stay within 1.5C, developed economies should phase out coal before 2030, rather than in the 2030s as in the deal announced on Wednesday night.

Elif Gündüzyeli, senior coal policy coordinator at the campaign group Climate Action Network Europe, said: "This is not a game-changer. A 2030 phaseout deadline should be a minimum, and this agreement doesn't have that. Coal is already expensive [compared with renewable energy] and no one wants to put money in coal any more."

The IEA has said all new development of fossil fuels must cease from this year, if the world is to stay within the 1.5C limit. The IEA's executive director, Fatih Birol, has also frequently called for the world to

	give up on coal, which produces more carbon than other sources of electricity, if the climate crisis is to be tackled. Although South Africa, Indonesia and the Philippines did not sign up to phase out coal, they agreed deals that will lead to the early retirement of many of their existing coal-fired power plans.
Return to Top	

HEADLINE	**11/03 Covid-19 does not infect human brain cells?**
SOURCE	**https://www.theguardian.com/world/2021/nov/03/covid-19-virus-does-not-infect-human-brain-cells-new-study-suggests**
GIST	The virus that causes Covid-19 does not infect human brain cells, according to a study published in the journal Cell. The findings will raise hopes that the damage caused by Sars-CoV-2 might be more superficial and reversible than previously feared. The study contradicts earlier research that suggested the virus infects neurons in the membrane that lines the upper recesses of the nose. This membrane, called the olfactory mucosa, is where the virus first lands when it is inhaled. Within it are olfactory sensory neurons (OSNs), which are responsible for initiating smell sensations. They are tightly entwined with a kind of support cell called sustentacular cells. In the new study, Belgian and German researchers claim that the virus infects sustentacular cells but not OSNs. “That is just a critical distinction,” said the senior author Peter Mombaerts, who directs the Max Planck Research Unit for Neurogenetics in Frankfurt, Germany. “Once you believe that olfactory neurons can be infected, there is a quick route into the olfactory bulb and then you’re in the brain already.” The olfactory bulb, at the front of the brain, is where neural input about odours is first processed. If the virus penetrated this structure it could theoretically spread to deeper brain regions where it could do lasting damage – especially since, unlike OSNs, most neurons are not regenerated once lost. But if the virus only infects the sustentacular cells, then the damage could be less long-lasting. Both pathways could explain the olfactory dysfunction that afflicts an estimated half of all Covid-19 patients. In one in 10 of those, the loss or change of smell is long-term, perhaps permanent. Mombaerts says this could be the result of support for the OSNs breaking down, even if they themselves are not infected. They may function below par, or stop functioning altogether, until the sustentacular cells regenerate. The group has not looked at other neurological symptoms of Covid-19, such as the fatigue and “brain fog” that accompany long Covid. Nobody doubts that the central nervous system is affected by the disease; the debate concerns whether these effects are due to the virus infecting neurons or some more indirect mechanism, such as an inflammatory response in the blood irrigating the brain – with different implications for prognosis and treatment. The findings are likely to prove controversial because of the difficulty of studying molecular events unfolding in the moments after infection. Earlier studies made use of animal models, clusters of neural stem cells grown in a dish, and postmortem tissue taken from small numbers of Covid-19 patients. The present study is the largest in Covid-19 patients to date, and it deployed a novel technique for capturing those early events. Laura Van Gerven, a neurosurgeon at the Catholic University of Leuven in Belgium and another of the paper’s senior authors, adapted a form of skull base surgery to remove tissue from the olfactory mucosa

	and bulb of Covid-19 patients within about an hour of their death. In 30 of the patients, the researchers were able to detect that the virus was still replicating – meaning the patients had died in the acute, contagious phase of the disease. "It is unquestionably the most thoroughly done bit of work on human postmortem olfactory Covid tissue," said Stuart Firestein, a neurobiologist at Columbia University in New York City. But Firestein said the results did not shed much new light on how Covid-19 causes olfactory dysfunction. "They do not show any OSNs as being damaged or there being fewer of them, or the OSNs near infected sustentacular cells as being different in any way from those not near infected cells," he said. Debby Van Riel, a virologist at Erasmus University in Rotterdam, the Netherlands, also praised the study's rigour, but said the authors' claim that Sars-CoV-2 does not infect neurons was "pretty bold". In only six of the 30 patients was the virus detectable in the olfactory mucosa itself. "Overall the numbers are thus really low to make any strong conclusions," she said. But even if the study isn't the last word on Covid's brain effects, it does indicate that those dire early reports weren't either. If its conclusions are borne out, those experiencing Covid-related anosmia or parosmia can be reassured that the virus has not infected their brains, and that future therapies targeting the understudied sustentacular cells could alleviate or cure their condition.
Return to Top	

HEADLINE	**11/03 Germany: pandemic of unvaccinated**
SOURCE	**https://www.theguardian.com/world/2021/nov/03/germany-enveloped-in-massive-pandemic-of-the-unvaccinated**
GIST	Germany's health minister, Jens Spahn, has warned that his country is going through a "massive" pandemic of the unvaccinated**.** "The pandemic is far from over," said Spahn, a member of the Christian Democratic Union (CDU). "We are currently experiencing a pandemic of the unvaccinated, which is massive. There would be fewer coronavirus patients on intensive care units if more people would let themselves be vaccinated." In the last week several German clinics have raised alarm about rising numbers of patients with Covid-19 on the wards. On Wednesday authorities reported 2,220 patients in intensive care beds, the highest number since the start of June. Over the last seven days 666 people have died from the virus in Germany, slightly more than in the same week a year ago, before the start of the vaccination drive and the arrival of the more infectious Delta variant. For now the number of fatalities is rising less steeply than it did during the previous three coronavirus waves in the country. The head of Germany's disease control agency, Lothar Wieler, described the recent rise in infection rates as frightening. "The fourth wave is developing in exactly the way we feared, because not enough people have received the vaccine," said Wieler, who is president of the Robert Koch Institute. The percentage of the German population fully vaccinated against Covid-19 has in effect flatlined for the last month at 66%, a lower rate than in other western European states such as France, Italy, Spain and the UK. Surveys suggest those who have refused a jab so far are unlikely to change their mind. A number of high-profile people such as the Bayern Munich footballer Joshua Kimmich and the former Die Linke chairperson Sahra Wagenknecht have recently made public that they have declined to be vaccinated.

	Unlike many of its southern European neighbours, Germany has not made vaccination mandatory for some professional sectors, such as care for elderly people, and on Wednesday Spahn reiterated that there were no plans to do so in the future. Instead, the health minister pointed to recent numbers from Israel as evidence that governments could get on top of a fourth wave of the pandemic by quickly administering booster shoots to those who had received their vaccinations more than six months ago. “A booster shot can make a real difference,” he said. However, Israel has a much higher percentage of the population already vaccinated, estimated at above 80%. In Germany’s federalised system, health authorities in each of the 16 states are responsible for setting up infrastructure that would allow vaccines to be administered en masse. Many of the vaccine centres set up at the start of the year have been in standby mode since September and would need to hire or train new staff to be reactivated. Leif Erik Sander, a physician at the department of infectious diseases and respiratory medicine at Berlin’s Charité hospital, said on Wednesday that about 30 million people in Germany were already or would soon be in need of a booster shot, but vaccinations were only happening at a rate of about 150,000 people a day. “It’s fairly easy to calculate that at this rate we wouldn’t be able to immunise these groups in time for this winter,” Sander said.
Return to Top	

HEADLINE	**11/03 Iran sets date to resume nuclear talks**
SOURCE	**https://www.theguardian.com/world/2021/nov/03/iran-sets-date-to-resume-talks-on-nuclear-deal-after-five-month-gap**
GIST	Iran has agreed to resume talks with world powers on reviving a nuclear deal on 29 November after a five-month gap, with the US urging a quick resolution. The announcement of indirect negotiations in Vienna comes as pressure mounts on Iran, with western nations warning that Tehran’s nuclear work is advancing to dangerous levels and Israel threatening to attack. The EU envoy Enrique Mora, who led six rounds of talks earlier this year and recently flew to Tehran to seek progress, will again chair the 29 November meeting, the EU announced. President Joe Biden took office hoping to return to the 2015 agreement from which his predecessor Donald Trump bolted. But the talks earlier this year failed to secure a breakthrough with Iran, which requested a pause after the June election of a new hardline president, Ebrahim Raisi. In Washington, state department spokesman Ned Price said the US believed it was possible to quickly resolve the “relatively small number of issues that remained outstanding at the end of June”. “We believe that if the Iranians are serious, we can manage to do that in relatively short order,” Price told reporters. “But we’ve also been clear, including as this pause has dragged on for some time, that this window of opportunity will not be open for ever.” Trump slapped sweeping sanctions on Iran as he withdrew the US in 2018, leading Tehran to take steps out of compliance with the deal through which it had been drastically scaling back sensitive nuclear work. Iran wants a lifting of all US sanctions but the Biden administration says that it will only negotiate about measures taken by Trump over the nuclear programme, such as a unilateral ban on oil sales, not steps imposed because of concerns such as human rights.

	Iran also wants commitments that the United States will stay committed to the deal – an unlikely proposition in Washington, where Trump's Republican party, emboldened by a state election win on Tuesday, fiercely opposes Biden's diplomacy with Iran. "The American president lacks authority and refuses to offer guarantees," Iran's top security official, Ali Shamkhani, wrote on Twitter as the talks were announced. "If that does not change, the result of the negotiations is already clear." The deputy foreign minister, Ali Bagheri, Iran's lead negotiator, confirmed the 29 November resumption of talks and said the goal would be "the removal of unlawful and inhumane sanctions". Adding to US frustrations, Iran has refused to meet directly with the US envoy, Robert Malley, so instead European mediators have to shuttle between hotels in Vienna. Britain, China, France, Germany and Russia remain in the deal with Iran and will take part in the negotiations, the EU statement said. European powers have increasingly voiced alarm at Iran's nuclear work during the standstill in negotiations, warning that Tehran's progress will be so advanced that a return to the agreement may be useless.
Return to Top	

HEADLINE	**11/03 Workers quitting in record numbers**
SOURCE	**https://www.theguardian.com/us-news/2021/nov/03/an-unbelievable-sense-of-freedom-why-americans-are-quitting-in-record-numbers**
GIST	Josie, 19, landed her first "adult" job as an IT support worker last November, just a few months after graduating from high school. Though the job could be done fully remotely, managers insisted that she come into the office – despite the pandemic. At first, her co-workers and managers wore masks, but often incorrectly; when the local mask mandate was lifted, people stopped wearing them altogether. "It was honestly scary," Josie recalls. She'd just moved into her first apartment with her partner; both have pre-existing health conditions that increase their vulnerability to severe illness from Covid-19. But as the sole earner in her two-person household, Josie felt resigned to the daily risk at work. "It was like getting shot out of a cannon into adulthood," she says. This August amid the rise of the Delta variant, she finally quit – becoming one of the 4.3 million American workers to voluntarily leave their jobs during that month alone. It was a record-breaking month for resignations since the government began tracking monthly job turnovers more than two decades ago, according to labor department data released in mid-October. Between January and August of this year, at least 30 million Americans quit their jobs. Whether you call it the "Great Resignation" or a "nationwide reassessment of work", the labor market shake-up of the pandemic could have unexpected aftershocks for years to come. That may be especially true for early-career workers like Josie, who have now spent a major chunk of their working lives under the strain of Covid-19. Many of these workers say their job experiences in the pandemic have led them to recognize their real priorities in life – and leaving a job is perhaps the boldest assertion of those priorities they can make. **'It gave me this unbelievable sense of freedom'**

“I never imagined it would happen this way, but here I am,” says Alex, a 27-year-old marketing professional who had worked at the same Boston-based consumer tech startup since she graduated from college until early October, when she resigned from the company via email.

Pre-pandemic, the company’s culture was relaxed. But the switch to fully remote work in March 2020 was swiftly followed by a sharp boom in product sales. Over time, an “always on” work culture crept in as a result, with co-workers communicating at all hours. When a colleague left the company, Alex’s workload doubled with no additional pay.

“I just felt like I couldn’t let things go, because [the company was] really small,” she says. “If anyone were to leave, it just seemed impossible.”

Alex reached out to teammates for help, only to discover that they were just as burned out as she was. But because this was the only job she’d ever had, she didn’t initially recognize that the extent of her overwork – and her sense of personal obligation to the business – were not necessarily normal or healthy. That is, until she talked to others outside the company.

Quitting has been more than a relief. “It gave me this unbelievable sense of freedom that I could do whatever I wanted, and made things so much clearer,” says Alex, speaking from her parents’ home near Washington.

She plans to spend a few months relaxing with family before finding a new job, possibly in non-profit work. She has also begun revisiting long-deferred plans to pursue a graduate degree in public administration – plans that were easy to neglect in the face of an ever-mounting workload.

Like Alex, 28-year-old Cassie also experienced a pandemic burnout in her role as a case manager for a life insurance company in central Pennsylvania. A visual artist by training, Cassie joined the firm in July 2019 after a stint doing freelance graphic design work. It wasn’t her dream job, but the stability was a nice change at first.

Then in the second half of 2020, her workload multiplied seemingly overnight. Before long, Cassie was fielding more work calls than any single person could handle. Work became so all-consuming that she converted her home studio space, originally set up for unwinding and making art, into a makeshift home office.

“[The pandemic] turned this space for good times into work times, and eventually bad times,” Cassie recalls.

While she remains grateful to have had the ability to work from home in 2020, losing the time and space for a creative outlet was a blow. A few weeks ago, she opted to leave the job for good. Thanks to a salaried live-in partner and some personal savings, she feels fortunate to have a “coasting budget” to live from while she explores what comes next. She hopes to find a job that’s both creative and stable.

‘My life is my life and my job is my job’

For 27-year-old Lloren Zeigler, quitting was a way to regain control of her time. Leaving her job as a television production manager, last December, was easy. “They wanted me to work through the holiday and I said abso-f**king-lutely not,” says Zeigler.

Since walking away from her entertainment industry role nearly a year ago, the Los Angeles-based Zeigler has devoted herself full-time to the small business she began in 2020 with her partner, Liz Sanchez. The pair make incense that they sell at local swap meets and flea markets under the brand Le Trois Apothecary. It may or may not become a forever-job, but Zeigler appreciates the opportunity to nurture her entrepreneurial streak.

Nancy, 30, a PR professional who also lives in Los Angeles, similarly resigned from her job for the greener pastures of self-employment. Working remotely during quarantine, she realized that she didn’t

	need to rely on a hovering boss to be productive and do work that she could feel good about. In October, she left her position at a small recording company after just three months – her second time quitting a job during the pandemic. "My job is not my life," Nancy says. "My life is my life and my job is my job. I'm willing to take on the uncertainty [of unemployment] simply to have my own time under control, and have my own life available to me." While Nancy remains open to the possibility of another full-time role, she says that a prospective employer would need to respect her boundaries and trust her to manage her own schedule. For the time being, she plans to pursue freelance music marketing projects and related project management. Josie, the 19-year-old in Ohio, is similarly protective of her personal boundaries in a work setting. Since quitting, she's found a new job doing similar work for a different company. This time, however, the position is fully remote. Though she isn't sure where her future will lead, Josie says she now knows what her rights are as a worker. They include the right to leave a job without remorse. "Companies don't care about me, either," she says.
Return to Top	

HEADLINE	**11/03 NYC mayor: young children vaccination**
SOURCE	**https://www.nytimes.com/live/2021/11/03/world/covid-delta-variant-vaccine#nyc-children-covid-vaccine**
GIST	Coronavirus vaccinations for children 5 to 11 years old are expected to begin Thursday in New York City, Mayor Bill de Blasio said on Wednesday. City officials said there were more than 230,000 pediatric doses of the Pfizer-BioNTech vaccine already on hand in the city or on their way. While other places in the country began vaccinating younger children Wednesday morning, New York City was still waiting for official clinical guidance from the Centers for Disease Control and Prevention for health care providers, before setting in motion its distribution plan for pediatric vaccine doses, Dr. Dave Chokshi, the city's health commissioner, said at a news conference. The guidance will include a safety checklist, he said, to make sure that providers take every precaution. "We are expecting that sometime today," Dr. Chokshi said, "and once that final piece is released, we will have all of the information that we need." The New York State Health Department said on Wednesday that providers could go ahead without waiting for the federal clinical guidance, but that it was also fine to wait for it to arrive. As a result, New York parents planning to get their children vaccinated at the earliest possible moment may still face some hurdles. As of Wednesday morning, the city and state vaccine finder websites were not yet showing appointments for children younger than 12. The Walgreens pharmacy chain, however, was allowing parents to schedule appointments for doses, as it is doing around the country. The city's public hospital system said it expected its online booking system for pediatric doses to go into service Wednesday night. And by the end of the week, the first of almost 1,500 pediatricians and family doctors across the city will begin administering vaccine doses to younger children, city officials said. New York State set up a special committee more than a year ago to provide an extra level of scrutiny for federal vaccine decisions. That committee met Tuesday night and signed off on administering pediatric doses of the Pfizer-BioNTech vaccine to children aged 5 to 11. But the associated paperwork, which includes safety guidelines, typically takes about 24 hours to be disseminated, said Dr. Bruce Farber, the chief of infectious disease at Northwell Health and a member of the committee. He said the paperwork delay did not have to be an impediment to starting vaccinations.

	"It has been approved, and will be up and running in a very short period of time," Dr. Farber said. Assuming the guidance arrives on schedule, parents and children in New York City will be able to walk in to city-run sites and sites run by the city's public hospital system on Thursday for shots. Appointments, however, are recommended. Appointments for next week at Walgreens locations in the city were being snapped up quickly. "Our children are precious to us," Mr. de Blasio said Wednesday. "Let's get them vaccinated, let's keep them safe, let's move out of the Covid era once and for all." The city's distribution plan will go into full swing next week. Next Monday, the city will begin hosting one-day vaccine clinics during school hours at each of its 1,070 schools that enroll children aged 5 to 11. A parent or guardian must either be present or give verbal or written consent for a child to receive a shot. Children 5 to 11 are now becoming infected at a higher rate, relative to their numbers, than any other age group in New York City, according to city data, a trend that arose with the start of school and peaked in late September. City officials said they now hope for the same success vaccinating them that they have seen with older children, 78 percent of whom have been immunized so far. "This is a significant turning point in our city's battle against this pandemic," said Mark Treyger, the chair of the City Council's education committee.
Return to Top	

HEADLINE	**11/03 Covid shots young children begin in Texas**
SOURCE	**https://www.nytimes.com/live/2021/11/03/world/covid-delta-variant-vaccine#covid-vaccine-children-texas-hospital**
GIST	HOUSTON — Surrounded by anxious and excited parents, the first young children in Texas — and some of the first in the nation — were vaccinated against the coronavirus early on Wednesday. The first two doses at Texas Children's Hospital went to Paxton Bowers, 5, a leukemia patient at the hospital, and his brother Patrick, 9, before the sun had risen. More than 35,000 children 5 to 11 have been signed up for shots at Texas Children's so far, and hundreds of them were expected to be immunized on Wednesday. The Centers for Disease Control and Prevention endorsed pediatric doses of the Pfizer-BioNTech coronavirus vaccine for children in that age group on Tuesday, a move that expands eligibility for the vaccine to 29 million younger Americans and will ease the worries of many pandemic-weary parents. The younger children get one-third of the vaccine dosage that has been cleared for adults and children 12 or older, delivered using smaller needles and different vials to minimize the chance of confusion with adult doses. About 2.9 million children aged 5 to 11 live in Texas. Twenty-two children in that age group have died from complications of Covid-19 in the state, and 118 have been diagnosed with Multisystem Inflammatory Syndrome in Children following a coronavirus infection, according to the Texas Department of State Health Services. At the hospital in Houston, the surroundings resembled vaccination sites nationwide, with some modifications for a younger crowd. Several support dogs roamed among the nurses. "The Little Mermaid" played on a large screen in the post-injection monitoring area, which was decorated with Disney-character balloons. Chairs were set up in pairs so that children could sit with a parent or caregiver.

	In the vaccination rooms, cheers mixed with yelps and a little bit of crying. Some children squirmed. Others jumped for joy. "This is the best day ever!" said Elizabeth Burke, a sixth grader who celebrated her 12th birthday on Wednesday by getting her shot. She was the youngest of three children in her family, and the last to get immunized. "We've kept her pretty isolated; we followed all the rules," said her mother, Lauren Burke. "She was really a trooper." Nearby, Camryn Zoë Emanuel, 8, a third grader, said she looked forward to being able to spend more time with friends. "Just have more hang-outs," she said. As for the shot, "it didn't hurt that much," she said, "but it kind of hurt." "She was real brave," said her mother, Sonja Emanuel, who brought her daughter in from the Houston suburb of Missouri City. "This is something she wanted." The hospital was also giving shots to parents who wanted a first dose or a booster. Ms. Emanuel sat for a booster after her daughter got her shot. "It's a relief," said Scott Solomon, who watched as his three children, 11, 9, and 6, all got vaccinated on Wednesday. "We went in birth order," he said. Thomas, his youngest, squirmed as the nurse prepared the shot. His mother, Catharina Solomon, held him on her lap. "We're doing this to protect you, bud," she said. "Thomas, look at the doggy!" Next to him sat a golden retriever comfort dog, his paws raised by the handler to give Thomas a pair of high-fives. Thomas cried. His brother Nicholas, 9, tried to talk him through it. Then the shot was over. "Dad, I get to punch you now!" Thomas said, standing up and walking over to Mr. Solomon. Then he showed the neon Band-Aid on his leg where the shot had gone in. He said it hurt a little, and now he was ready for a treat. "I'm going to get a doughnut," he said.
Return to Top	

HEADLINE	**11/03 Iran seizes oil tanker; ownership dispute?**
SOURCE	**https://www.nytimes.com/2021/11/03/world/middleeast/iran-tanker-oil.html**
GIST	American and Iranian officials both said Wednesday that Iran had seized an oil tanker in the Sea of Oman last month after an encounter with the U.S. Navy, but the two sides gave widely differing accounts of whose tanker it was and what, exactly, had happened. Iranian officials said the United States had seized a tanker carrying Iranian oil on Oct. 24 and that an assault by Iranian commandos had taken the tanker back. A statement by the Islamic Revolutionary Guards Corps said that "the brave I.R.G.C. naval unit landed on the tanker that had the stolen oil, seized it and brought it back to Iranian waters." Two U.S. officials, who spoke on condition of anonymity to discuss confidential intelligence assessments, said that Iran had seized a Vietnamese-flagged tanker, the MV Southys.

A U.S. Navy destroyer, The Sullivans, arrived to monitor the seizure but took no action and was not threatened by approaching Iranian speedboats, one of the officials said.

John F. Kirby, the chief Pentagon spokesman, denied Iran's allegations that the United States had seized the merchant vessel, whose nationality he declined to identify.

"It's a ridiculous claim," he told reporters in Washington. "It's absolutely not true. And I would add that Iran's actions, the ones that are true of them, illegally boarding and seizing a merchant vessel, constitute a blatant violation of international law."

Reports on social media accounts affiliated with the Revolutionary Guards gave yet another version of the story, the latest episode in a long-running tit-for-tat series of maritime skirmishes between Iran and the West. This version of events was endorsed by two Iranians with knowledge of the incident.

They said the seized tanker was one of four tankers carrying Iranian oil to Venezuela that had been seized by the United States in the Atlantic Ocean in August of last year.

Iranian officials, they said, had been waiting ever since for the tanker to come near its shores to take it back.

"Now the tanker with the same captain & crew & under US military protection has been seized by the IRGC Navy," Seyed Mohammad Marandi, a Tehran-based analyst close to the government, said in a tweet.

An Iranian oil dealer with knowledge of the incident confirmed that account. He said Iran had retaliated to demonstrate that seizing its oil in international waters would not go unanswered.

Similarly, Iran seized a British tanker in 2019 in response to the confiscation of an Iranian oil tanker by British forces near Gibraltar.

The ship seized last month was being held at Bandar Abbas and the crew was in custody, Iran's state media said.

A Pentagon spokesman rejected the claim that the tanker was one that had been seized by the United States last year.

"The vessel at the center of the 24 Oct. seizure by Iranian forces was NOT one involved in the Iran-Venezuela situation 8 months ago," Maj. Rob Lodewick said in an email.

A person who answered the phone at the Vietnamese Embassy in Washington declined to comment.

It was unclear why the seizure of the tanker was just coming to light on Wednesday.

The United States had not publicized the event, one American official said, because of current diplomatic sensitivities with Iran.

"If you're asking me, why am I talking about this today, because the Iranians lied about it today," Mr. Kirby said. "But we monitor maritime traffic every day out there, and not all of it rises to the level of us putting out a press release."

Indirect talks between the United States and Iran over resurrecting the 2015 nuclear agreement have been stalled for months.

Iran's Foreign Ministry announced Wednesday that the talks would resume on Nov. 29 in Vienna.

	Iran may have announced the seizure Wednesday, and played up the ostensible confrontation with the Americans, because it was the day before the 42nd anniversary of the 1979 Iranian takeover of the American embassy, an event that Iran celebrates annually with pomp and ceremony. Iran's state media cast the tanker incident as a bravura action by the Revolutionary Guards Special Forces, which chased U.S. warships away by "locking on missiles" at the ship and warning its crew to leave the area or face military confrontation. A dramatic video broadcast on state television, ostensibly of the Oct. 24 seizure, showed Iranian commandos boarding a helicopter and landing on a tanker with machine guns pointed at the crew. Several speedboats circled the tanker and a voice in English warned a U.S. ship to leave the area. One of the American officials dismissed that account, saying that some Revolutionary Guard speedboats approached The Sullivans but were not threatening. He described it as just some "sporty activity" between the Guards and the Navy ship. Separately, a U.S. official said Wednesday that multiple drones, believed to be Iranian, had "unsafe and unprofessional interaction" with the U.S.S. Essex aircraft carrier as the vessel left the Strait of Hormuz within the past 24 hours. The drones flew close to the Essex, interfering with the ship's flight operations prompting it to take defensive measures, defusing the encounter, the official said.
Return to Top	

HEADLINE	**11/03 Payments to separated migrants rejected**
SOURCE	**https://www.nytimes.com/2021/11/03/us/politics/biden-rejects-payments-migrants.html**
GIST	WASHINGTON — President Biden on Wednesday said migrants separated from family members at the border would not receive hundreds of thousands of dollars for the damage inflicted by the Trump-era policy, rejecting an option for monetary compensation that had been floated in negotiations with lawyers representing the families. Representatives of the migrant families and government officials had discussed giving families $450,000 for each member affected by former President Donald J. Trump's "zero tolerance" policy, which led to the separation of about 5,500 children from their parents, according to people familiar with the matter. But when asked on Wednesday about compensating the migrants, Mr. Biden denied the option was on the table. "$450,000 per person? Is that what you're saying?" Mr. Biden said when asked by Fox News reporter Peter Doocy about the payments. "That's not going to happen." Mr. Biden made the comment as he took questions after touting the forthcoming availability of vaccines for children. The remark was swiftly condemned by the American Civil Liberties Union, which is negotiating on behalf of the separated families. "If he follows through on what he said, the president is abandoning a core campaign promise to do justice for the thousands of separated families," Anthony Romero, the executive director the A.C.L.U., said in a statement. "We respectfully remind President Biden that he called these actions 'criminal' in a debate with then-President Trump, and campaigned on remedying and rectifying the lawlessness of the Trump administration." Mr. Romero also acknowledged that Mr. Biden may have been caught off guard by the question and may not have been aware of the details of ongoing negotiations with the Justice Department.

	The comments, however, also amounted to the second time in recent weeks the president has spoken about pending Justice Department actions. After Mr. Trump repeatedly interfered in the department's affairs, Mr. Biden made restoring independence to the agency one of his goals. Asked about the president's comment on Wednesday, Dena Iverson, a spokeswoman for the Justice Department, said "the department will not comment on ongoing litigation." Mr. Biden said last month that the Justice Department should prosecute those who defy subpoenas from the House committee investigating the Jan. 6 attack on the Capitol, a comment he later walked back during a CNN town hall. "The way I said it was not appropriate," Mr. Biden said. In the negotiations with the administration, which were first reported by The Wall Street Journal, lawyers representing the migrants have argued that the United States government wronged the families by separating parents from children. In addition to financial compensation, the A.C.L.U. is also trying to reach a settlement with the government that would provide, among other things, a pathway for the families to remain in the United States and receive social services. The Biden administration's handling of rising illegal border crossings has received criticism from Democrats and Republicans alike. To contend with the record number of crossings, Mr. Biden has continued to use a Trump-era border policy that rapidly turns away many migrants at the border without providing them a chance to ask for asylum in the United States. The administration has said the policy is necessary to contain the ongoing pandemic. The deterrent approach has also prompted fierce debate within the administration, with some of Mr. Biden's top aides favoring stronger policies to contain the crossings, while others support a more welcoming stance to make good on the president's campaign pledge of restoring an asylum program at the southwest border.
Return to Top	

HEADLINE	**11/03 Study: Russia implicated Ukraine conflict**
SOURCE	**https://www.nytimes.com/2021/11/03/world/weapons-ukraine-russia.html**
GIST	KYIV, Ukraine — A study of weapons and ammunition used in the war in Ukraine shows that Russia has been systematically fanning the conflict with arms shipments, according to a new report funded by the European Union and the German government. The study is hardly the first to reach this conclusion: the United States and European countries have sanctioned Russia for years for arms transfers to separatist forces they say Moscow is supporting in Ukraine. But the study is one of the most comprehensive to date on the issue. While unlikely to change the overall picture, it offered a fine-grained view of illicit weapons transfers in Ukraine and illustrated the scope of the arms trade that is fueling Europe's only active war. Earlier analyses of Russian weapons transfers in Ukraine leaned on photographs or government intelligence. The new report focused on actual armaments. Researchers studied dozens of rifles, grenade launchers, shoulder-fired antiaircraft missiles and thousands of rounds of ammunition taken from captured or killed separatist fighters or positions they had occupied. The researchers examined the recovered weapons and traced serial numbers and other identifying marks back to manufacturers. It provided "a window into a largely forgotten conflict that, since early 2014, has persisted on the edge of Europe," the report said.

Titled “Weapons of War in Ukraine,” the report said that the separatist forces “are more than militias armed with weapons inherited from the former Soviet Union; rather, they mimic modern armies and follow established military doctrine.”

The war, fought along an about 280-mile-long trench line that cuts through the flatlands of eastern Ukraine, began after street protesters deposed a pro-Russian Ukrainian president in 2014. Russia responded with a military intervention it has never acknowledged.

The Kremlin has consistently denied transferring arms to Ukraine, even after Western governments documented major weaponry crossing the border. This included a tracked vehicle-mounted antiaircraft missile system that shot down a civilian airliner in 2014, killing all 298 people aboard. Russian officials have blamed Western governments for fomenting the conflict with military support for the Ukrainian government, including the United States’ provision of anti-tank Javelin missiles and Turkey’s supply of Bayraktar armed drones, used for the first time in conflict just last month.

The conflict has again raised alarms this fall. Commercial satellite photographs and videos posted on social media have shown Russian tanks and other armored vehicles close to the Ukrainian border, raising fears of a direct invasion.

And the volume of arms transfers to proxy forces already in Ukraine outlined in the new report highlights the volatility of the situation. The study, conducted by Conflict Armament Research, a company based in Britain that specializes in tracing weaponry, was funded by the European Union and the German Federal Foreign Office.

The study looked largely at small arms, the most basic but often most lethal weapons in wars even when more sophisticated armaments are in use, as is the case in Ukraine.

The study found weaponry that the researchers suggested could have come from nowhere but Russian military arsenals. It found, for example, several types of grenade launchers, sniper rifles and land mines that were never in service with the Ukrainian military, and hence could not have been captured and put to use by the separatist armies. Specialized weaponry also turned up. The researchers say they documented a Russian factory-made “anti-handling” device, or booby-trap, that can be set under a land mine to go off when someone tries to disarm the mine.

More subtle evidence also pointed to separatists having a direct line of support from Russia.

Kalashnikov rifles found in illicit small-arms trade in developing world conflicts, where they are the work-a-day weapon of many militant groups, are typically assembled from parts from multiple guns, the report noted. Mismatched serial numbers on components is common. But that was not the case in eastern Ukraine, the report said: the rifles had matching parts, suggesting a more direct route from factory to battlefield.

The study traced 4,793 rounds of small-arms ammunition and 43 weapons recovered from battlefields from 2014 until 2019. Analysts traced ammunition using “headstamps” or the stamped markings ringing the primers on casings, and weapons by serial numbers. The Russian government and Russian arms manufacturers did not respond to the researchers’ requests for comment.

Though clinical in tone, the report did hint at the grim human drama behind the items being studied.

A rifle that once belonged to a separatist soldier, for example, arrived in front of the British researchers still tied with a ribbon inscribed with Orthodox Christian prayers for protection.

The study of bullets painted a more nuanced picture on sourcing. The entire sample of small-arms ammunition had been manufactured at sites in what is now Russia, the researchers said. The prevalence of a caliber of ammunition used in Kalashnikovs only after 1974 suggested a more modern arsenal. But much had been in storage for years, leaving its provenance uncertain.

	The bullets looked at in the study were made over a span of 65 years, the oldest being a round for a Kalashnikov made in 1948, just a year after the rifle was first introduced in the Soviet Union.
Return to Top	

HEADLINE	**11/03 Ethiopia leader defiant as rebels advance**
SOURCE	**https://www.nytimes.com/2021/11/03/world/africa/ethiopia-war-un-report.html?action=click&module=Well&pgtype=Homepage&section=World%20News**
GIST	NAIROBI, Kenya — As rebel fighters drew closer to the capital on Wednesday, Ethiopia's embattled leader appealed to his soldiers to defend the city "with our blood," in a stark and inflammatory speech that heightened the mounting air of crisis in Africa's second-most populous country. "We will sacrifice our blood and bone to bury this enemy and uphold Ethiopia's dignity and flag," Prime Minister Abiy Ahmed said at the military headquarters in the capital, Addis Ababa, a day after he had declared a national state of emergency and called on Ethiopians to pick up arms and repel approaching forces from the northern Tigray region. Mr. Abiy, the winner of the 2019 Nobel Peace Prize, made his comments as the top United Nations human rights body released a report that offered more evidence of gross human rights violations by all sides in the year-old conflict, including massacres of civilians, sexual violence and attacks on refugees. The Addis Ababa police continued a sweeping roundup of ethnic Tigrayans, raiding homes and cafes and checking identity cards on the street. The authorities claimed to be hunting for infiltrators, but analysts worried that, along with Mr. Abiy's heated talk, the detentions could foster ethnically motivated attacks in the city. The United States Embassy has advised American citizens in Ethiopia to leave immediately, and on Wednesday, it requested that Washington allow diplomats' families and nonessential staff to depart the country on a voluntary basis, said a senior official who was not authorized to speak publicly. The State Department, troubled by what it termed "the expansion of combat operations and intercommunal violence" there, said it was dispatching its Horn of Africa envoy, Jeffrey Feltman, to arrive in Ethiopia on Thursday. Alarm started to spread through the capital over the weekend, after Tigrayan rebels captured two major towns about 160 miles to the north, following weeks of battle against Ethiopian government troops and allied ethnic Amhara militias. The Tigrayans have joined forces with a smaller rebel group, from the ethnic Oromo group, and are preparing to prepare a major push toward Addis Ababa, a spokesman for the Oromos said on Wednesday. Mr. Abiy vowed to meet them with fire. "The enemy is digging a deep pit — a pit that will not be where Ethiopia will disintegrate, but where they will be buried," he said during a candle-lit ceremony at the military academy marking one year since the war in Tigray erupted. International pressure to halt the fighting, which has been accompanied by reports of rape, massacres and ethnic cleansing, has completely failed. Efforts to bring even a modicum of accountability for those atrocities have also come to little, as evidenced by the United Nations report released Wednesday. Presenting a document packed with disturbing testimony from victims and witnesses, the United Nations' human rights chief, Michelle Bachelet, said it pointed to "appalling levels of brutality" in the Tigray war that amounted to war crimes.

But the report by the U.N. body, which conducted the inquiry along with an Ethiopian government human rights commission, was written under significant government restrictions that critics said forced it to pull its punches. Ms. Bachelet said her team members had been subjected to intimidation and harassment during their research, and one was expelled on charges of "meddling in internal affairs."

The investigators were unable to visit several sites where serious violations were said to have occurred and did not include testimony from any of the 60,000 Ethiopian refugees at camps in Sudan.

The final report stopped short of saying which side had committed the most atrocities, and rights groups protested that it engaged in false equivalence — appearing to equate the atrocities committed by Tigrayan forces, mostly in the early weeks of the fight, with a far greater number of serious crimes by Ethiopian forces and their allies over the next eight months.

Even so, it was the first official account of the litany of horrors in the war, which erupted in November 2020 after a simmering political feud between Mr. Abiy and Tigrayan leaders. After Tigrayan troops attacked a federal base in the region, government troops launched an offensive. They were quickly bolstered by fighters crossing the border from Eritrea, the neighboring country to the north.

A woman abducted from a bus described being gang-raped over 11 days by 23 Eritrean troops who left her for dead. Witnesses said that Tigrayans armed with axes and machetes killed 200 ethnic Amhara civilians over two days in western Tigray.

Days later, they said, Amhara fighters arrived to carry out revenge killings.

An older man said he was among 600 Tigrayan men paraded naked through a village by Eritrean troops who mocked and photographed them.

Ms. Bachelet denied that her team had been swayed by the Ethiopian government, whose federal human rights body jointly investigated and wrote the report.

"Of course it is impartial," she said. "The report stands for itself. I can say it was done very seriously."

Human Rights Watch welcomed the report but said that it was "not an exhaustive account" of wartime atrocities in Ethiopia, and that a more thorough, independent inquiry was needed.

While most accounts of atrocities in Tigray have focused on Ethiopia and Eritrean troops and their allies, the U.N. report also lays out stark abuses by Tigrayan forces.

It described members of a Tigrayan youth group known as Samri going house to house in the town of Mai Kadra in November, slaughtering ethnic Amharas and other minorities and looting their property.

Although the report does not quantify the scale or proportion of atrocities committed by either side — in other words, who bore greater blame — Ms. Bachelet, during a news briefing, did point to Eritrean and Ethiopian troops.

The report also said it "could not confirm" the use of starvation as a weapon of war in Tigray. Yet other U.N. bodies have loudly criticized a de facto government blockade in place since July that has largely cut off food and medicine supplies to a region where 5.2 million people urgently need help and 400,000 are said to be living in faminelike conditions.

Ms. Bachelet, though, did not shy from describing the harsh effect of that blockade — no aid trucks have been allowed to enter Tigray since Oct. 18, she said. But that only raised questions about why such information had been excluded from the report.

Several Western diplomats familiar with the work of the U.N.-led investigation acknowledged its limitations, but said they hoped it might establish a foundation for future criminal prosecutions.

	Yet the report fails to identify individual perpetrators, and Ethiopia's judicial system has a poor record in bringing such cases to light. The authorities say they have convicted seven soldiers of rape and put another 20 on trial, Ms. Bachelet said. But those proceedings lacked transparency and did not meet international standards, she added. She said she supported the creation of an international investigative body for Ethiopia along the lines of those already working on war crimes and atrocities in Syria and Myanmar.
Return to Top	

HEADLINE	**11/03 Greece tightens restrictions unvaccinated**
SOURCE	**https://www.nytimes.com/2021/11/03/world/europe/greece-covid-restrictions.html**
GIST	As Greece broke another record in daily coronavirus infections this week, registering 6,700 new cases within the past 24 hours, the country's health minister announced a series of new restrictions aimed at flattening the spike. The restrictions, which are to apply from Saturday, relate to unvaccinated people, said the health minister, Thanos Plevris. All unvaccinated workers — except those who work from home exclusively — must undergo two Covid-19 tests per week. A negative rapid or PCR test will also be required from unvaccinated people who want to access public services, banks, shops and hair salons. The same will apply at cafes and restaurants, which are allowed to serve the unvaccinated outdoors. The rules will not apply to supermarkets, pharmacies and churches. The authorities will also intensify inspections and boost fines on businesses that violate regulations, increasing the minimum fine to 5,000 euros, from 1,000, Mr. Plevris said. In addition, in a bid to boost a lagging vaccination drive, the government is launching a campaign to win over the unvaccinated, sending text messages to mobile phones and running notices in the media extolling the benefits of the vaccine. "Our key weapon in this phase of the campaign is the vaccine," Mr. Plevris said, adding that "the more intense restrictive measures" imposed earlier in the pandemic were not an option, apparently referring to nationwide lockdowns. The announcements came as Greece experiences a sharp upturn in its daily infection rate, breaking record after record: 4,696 on Saturday, 5,449 on Monday and 6,700 on Tuesday. Last month the government lifted some pandemic restrictions, chiefly for vaccinated people, in regions where coronavirus cases have been the highest. In late September and early October, the daily infection rate appeared to have stabilized at around 2,000 new cases per day but started edging up late last month. Greece — a nation of 10.7 million, where six in 10 people have been fully vaccinated — enjoys a vaccination rate similar to the rest of Europe. Mr. Plevris, the health minister, said on Tuesday that 63 percent of the general population has been fully vaccinated. The corresponding rate for the European Union is 64.3 percent, according to the vaccine tracker of the European Center for Disease and Control. But other E.U. states have applied tougher restrictions on the unvaccinated. Italy has some of the bloc's most stringent regulations, notably the Green Pass, a mandatory health certificate for Italian workers which has fueled violent protests across the country. France has introduced a similar pass, which has also met with vehement public opposition. Protests in Greece have been regular but relatively small in size. On Wednesday, a rally in Athens against mandatory vaccinations for health workers drew a few hundred demonstrators.
Return to Top	

HEADLINE	**11/03 Fed steps toward end pandemic measures**
SOURCE	**https://www.nytimes.com/2021/11/03/business/economy/fed-taper-bond-buying.html**
GIST	The Federal Reserve on Wednesday took its first step toward withdrawing support for the American economy, saying that it would begin to wind down a stimulus program that's been in place since early in the pandemic as the economy heals and prices climb at an uncomfortably rapid pace. Central bank policymakers struck a slightly more wary tone about inflation, which has jumped this year amid booming consumer demand for goods and supply snarls. While officials still expect quick cost increases to fade, how quickly that will happen is unclear. Fed officials want to be prepared for any outcome at a time when the economy's trajectory is marked by grave uncertainty. They are not sure when prices will begin to calm down, to what extent the labor market will recover the millions of jobs still missing after last year's economic slump, or when they will begin to raise interest rates — which remain at rock-bottom to keep borrowing and spending cheap and easy. So the central bank's decision to dial back its other policy tool, large-scale bond purchases that keep money flowing through financial markets, was meant to give the Fed flexibility it might need to react to a shifting situation. Officials on Wednesday laid out a plan to slow their $120 billion in monthly Treasury bond and mortgage-backed security purchases by $15 billion a month starting in November. The purchases can lower long term interest rates and prod investors into investments that would spur growth. Assuming that pace holds, the bond buying would stop altogether around the time of the central bank's meeting next June — potentially putting the Fed in a position to lift interest rates by the middle of next year. The Fed is not yet saying that higher rates, a powerful tool that can swiftly slow demand and work to offset inflation, are imminent. Policymakers would prefer to leave them low for some time to allow the labor market to heal as much as possible. But the move announced on Wednesday will leave them more nimble to react if inflation remains sharply elevated into 2022 instead of beginning to moderate. Many officials would not want to lift interest rates while they are still buying bonds, because doing so would mean that one tool was stoking the economy while the other was restraining it. "We think we can be patient," Jerome H. Powell, the Fed's chair, said of the path ahead for interest rates. "If a response is called for, we will not hesitate." Congress has given the Fed two jobs: achieving and maintaining stable prices and maximum employment. Those are tricky tasks in 2021. Twenty months into the global coronavirus pandemic, inflation has shot higher, with prices climbing 4.4 percent in the year through September. That is well above the 2 percent price gains the Fed aims for on average over time. At the same time, far fewer people are working than did before the pandemic. About five million jobs are missing compared to February 2020. But that shortfall is hard to interpret, because businesses across the country are struggling to fill open positions and wages are quickly rising, hallmarks of a strong job market. For now, the Fed is betting that inflation will fade and the labor market will lure back workers, who might be lingering on the sidelines to avoid catching the coronavirus or because they have child care or other issues that are keeping them at home. "There's room for a whole lot of humility here," Mr. Powell said, explaining that it was hard to assess how quickly the employment rate might recover. "It's a complicated situation." Officials have already been surprised this year by how much inflation has surged and how long that pop has lasted. They had expected some run-up in prices as the cost of dining out and air travel bounced back

from pandemic-lockdown lows, but the severity of the supply chain disruptions and the continued strength of consumer demand has caught Fed officials and many economists by surprise.

In their November policy statement, Fed officials predicted that this burst of inflation would fade, but they toned down their confidence on that view. They said previously that factors causing elevated inflation were transitory, but they updated that language on Wednesday to say that the drivers were "expected to be" transitory, acknowledging growing uncertainty.

"Supply and demand imbalances related to the pandemic and the reopening of the economy have contributed to sizable price increases in some sectors," the statement added.

The Fed is willing to tolerate a temporary bout of quick inflation as the economy reopens from the pandemic, but if consumers and businesses come to expect persistently higher prices, that could spell trouble. High and erratic inflation that persists would make it hard for businesses to plan and might eat away at wage increases for workers who lack bargaining power.

"We have to be aware of the risks — particularly now the risk of significantly higher inflation," Mr. Powell said. "And we have to be in position to address that risk should it create a threat of more-persistent, longer-term inflation."

Investors were well prepared for Wednesday's announcement and took the news that bond buying will slow in stride. The S&P 500 rose 0.7 percent by the end of trading, reaching a new high.

That's notable because of the market's tumultuous reaction in 2013, when the Fed hinted that it would soon end a similar program that had been put in place in response to the financial crisis. A repeat of what came to be known as the "taper tantrum" in financial markets appears to have been avoided through the Fed's ginger communication in recent months.

Mr. Powell said the Fed would be "very transparent" if it should decide to speed or slow the pace of its winding down of the bond purchases, noting that it did not want to surprise markets.

"They're giving themselves the maximum amount of flexibility," said Seema Shah, chief strategist at Principal Global Investors, of Wednesday's statements from the Fed. "In fairness, this is a really uncertain environment, right? And there are things going on which are driving the economy which are really out of the Fed's control. So they can only try to be responsive."

Officials have tried to separate their path for slower bond buying from their plans for interest rates. But investors increasingly expect rate increases to start midway through 2022.

The Fed has said that it wants to achieve full employment before raising borrowing costs to cool the economy, and Mr. Powell was clear that the job market has yet to meet that milestone. He said it is possible, but not certain, that it could reach maximum employment next year.

If the Fed has to lift interest rates to contain inflation before the labor market is healed, it could come at a serious cost. While some employees may have retired since the onset of the pandemic, many people who are now sidelined are in their prime working years. They may start searching for jobs again as child-care issues are resolved and health concerns wane.

If the Fed slows the economy before they can, it could be harder for those workers to move into new jobs, leaving the economy with less potential and families with fewer paychecks.

"We're accountable to Congress and the American people for maximum employment and price stability," Mr. Powell said, noting that the pace of inflation right now is not consistent with price stability, but that the economy is also not at maximum employment.

He called the Fed's stance a "risk management" approach.

	"He acknowledged that there is a lot of uncertainty around the outlook right now," said Laura Rosner-Warburton, senior economist at MacroPolicy Perspectives. "Policy needs to have flexibility."
Return to Top	

HEADLINE	**11/03 Vaccinations for millions eligible children**
SOURCE	**https://www.nytimes.com/live/2021/11/03/world/covid-delta-variant-vaccine#biden-covid-vaccine-kids**
GIST	President Biden on Wednesday urged millions of parents to get their young children vaccinated against the coronavirus, touting the government's authorization of inoculations for children between 5 and 11 as a major milestone in the nation's effort to end the pandemic. Mr. Biden's comments came a day after the Centers for Disease Control and Prevention endorsed the Pfizer-BioNTech coronavirus vaccine for children. The decision was in sync with the Food and Drug Administration, which on Friday authorized emergency use of pediatric doses for the roughly 29 million children in that age group. "For parents all over this country, this is a day of relief and celebration," Mr. Biden said, adding that the vaccination program was ramping up this week with more doses being shipped out each day, to be "fully up and running by next week." Immunizing children 5 to 11 is expected to prevent about 600,000 new coronavirus cases between now and March 2022. Rising immunity may reduce the chances that young children will transmit the virus to vulnerable adults in their families and communities, health officials noted. It will also probably keep schools open. Jeffrey D. Zients, the White House's Covid-19 response coordinator, emphasized again at a news conference earlier on Wednesday that the rollout was still emerging, promising that millions more pediatric doses would be "in the air and on trucks" in the next 24 hours. By next week, he said, around 20,000 sites would offer the pediatric vaccine, with more coming in the weeks after. Mr. Zients said that state and municipal health departments would conduct thousands of community clinics at fairgrounds, zoos and sporting events, and that schools would host thousands of their own clinics this year. "I know many parents have been waiting for this day, but I also know some people might have some questions," Mr. Biden said, encouraging parents to speak to local doctors and community leaders about vaccination. The president said many of the vaccine sites would offer times at night and on weekends for parents to take their children for shots after work and after school. "This vaccine is safe and effective," Mr. Biden said. "So get your children vaccinated." One key resource was still missing from the administration's rollout: a way to find pediatric doses on vaccines.gov, the federal website that helps people locate vaccine availability near them. Asked why the administration had yet to program the site to find pediatric doses, Mr. Zients said that the site would do so by Friday. "You need to get the vaccines to the sites — the sites have to be ready and up and running," he said. "We'll have a threshold number of sites online by Friday."
Return to Top	

HEADLINE	**11/03 WHO authorizes India vaccine Covaxin**
SOURCE	**https://www.nytimes.com/live/2021/11/03/world/covid-delta-variant-vaccine#covaxin-covid-vaccine-who**

GIST	The World Health Organization on Wednesday granted emergency authorization to Covaxin, the first coronavirus vaccine developed in India and to get the designation, providing a major boost for Prime Minister Narendra Modi, who has stressed his intention of making the country's pandemic prevention effort self-reliant. The vaccine was developed by Bharat Biotech, an Indian drug company, and the Indian Council of Medical Research, a government body, and is the eighth coronavirus vaccine to receive the global health body's green light. The W.H.O. said in a tweet that Covaxin met standards for protection against Covid-19 and that the benefit of the vaccine far outweighs the risks. Mr. Modi's government was already exporting the vaccine to gain favors in a geopolitical struggle with China, which has used its large infrastructure projects to bolster its image. The W.H.O. said Covaxin had a 78 percent efficacy rate against Covid-19 and should be administered in two doses four weeks apart to adults, noting the vaccine's easier storage requirements might be convenient for poor and developing countries. On Wednesday, India's top drug regulatory authority said that it was extending the shelf life of Covaxin from 6 to 12 months from the date of manufacture, based on data showing that it is safe and effective. Mr. Modi, who got his first shot of the vaccine in March, said at the Group of 20 summit in Rome last week that his country will be able to produce over five billion vaccine doses overall next year to help the world in the fight against the pandemic. Covaxin was approved by Indian government officials in January and administered to millions of people even without data being released. Many in the country, including frontline health care workers, had feared that Covaxin could be ineffective or worse, slowing down the national campaign to inoculate 1.3 billion people. Officials in Brazil, where the government had bought doses of Covaxin, had raised questions about the vaccine and were investigating possible irregularities in its contract to buy 20 million shots of Covaxin from India. Covaxin is being manufactured in three different locations in India, with the current production at over 50 million doses per month. The company has said it is aiming to make 1 billion doses per year by the end of this year. The W.H.O.'s sign-off comes after a lengthy review period; the manufacturers applied in April and provided the first batch of data to the agency on July 6, addressing a host of issues, including the vaccine safety and efficacy. Covaxin's manufacturers said in a statement on Wednesday that the W.H.O.'s validation would help expedite requests from countries seeking to buy the vaccine. Dr. Krishna Ella, a top official at Bharat Biotech, said that the organization has focused on maintaining stringent quality and safety standards. The authorization "will enable us to contribute to accelerating the equitable access of Covid-19 vaccine, and the access to our vaccine globally," he said. Worldwide, about 75 percent of all Covid shots have been administered in high- and upper-middle-income countries, according to the Our World in Data project at the University of Oxford. Only 0.6 percent of doses have been administered in low-income countries.
Return to Top	

HEADLINE	**11/03 WHO urges countries hold off on boosters**
SOURCE	**https://www.nytimes.com/live/2021/11/03/world/covid-delta-variant-vaccine#latin-america-pressed-on-vaccine-priorities**
GIST	Officials from the World Health Organization on Wednesday urged countries in Latin America and the Caribbean to limit administering booster shots and hold off on vaccinating children, allocating scant doses to the most vulnerable. "In some countries, we have seen vaccine doses reaching all levels of the population before a high percentage of vulnerable" residents have been fully immunized, Dr. Jarbas Barbosa, assistant director of the Pan American Health Organization, a division of the W.H.O., said at a news conference. Just 46 percent of people in Latin America and the Caribbean have been fully vaccinated so far, with supplies being slow to reach many countries, the organization said. Inequities have plagued the region, too. While Chile and Uruguay have vaccinated more than 75 percent of their populations, countries like Haiti and Nicaragua have administered two jabs to less than 20 percent of people. Against this backdrop, vaccine supplies across the region must be distributed carefully and strategically, with the aim of reducing mortality and transmission of the virus among the adult population, Dr. Barbosa said. "P.A.H.O. urges countries to prioritize the elderly, frontline workers and people with pre-existing conditions — to protect them, but also to prevent the health system from becoming overburdened with severe cases," he said. Offering vaccines to children and booster shots to others before high-risk groups are fully vaccinated — as the Dominican Republic has done — "may be defusing some of the efforts" to control the virus in the region, Dr. Barbosa added. Still, echoing a recent W.H.O. recommendation, he stressed that older and immunocompromised people who received the Chinese-made vaccines Sinopharm or Sinovac Biotech will need a third shot to ensure they are fully protected against Covid-19. "Their vaccination cannot be considered complete until they have received their third shot," said Dr. Barbosa, noting that there is no evidence that healthy adults who have received two doses need another. This could affect millions of people in Latin America and the Caribbean, where many countries — including Chile and Brazil — have relied heavily on the more readily available Chinese-made shots to speed up vaccination. Vaccine supplies distributed through the United Nations-backed Covax program, meanwhile, are picking up pace, with Latin America and the Caribbean receiving around 64.3 million doses so far. Some 2.6 million doses have reached Venezuela, where the health system is especially fragile, and more supplies are expected in November. New Covid-19 cases across Latin America and the Caribbean have been declining in recent weeks, offering an encouraging signal for the region, Dr. Barbosa noted. But he urged countries to stay vigilant and maintain public health measures, warning that the pandemic is not over. "The declining case indices show that our approach is working," he said. "And it is critical for all of us to stay the course until everyone is vaccinated and protected from the virus." Officials also warned about the possibility of a spike in infections with the onset of winter and the holiday season. As travel restrictions are lifted in many countries, tourism could pose an additional risk, said Dr. Sylvain Aldighieri, the Covid-19 incident manager at P.A.H.O.

	"Social distancing and avoiding closed environments, together with mask wearing, are the most important tools for limiting the transmission," Dr. Aldighieri said. "The public really has to incorporate these basic measures into their lifestyle, including beach, seaside and vacation activities."
Return to Top	

HEADLINE	**11/03 Colorado hospitals nearly full; virus wave**
SOURCE	**https://www.nytimes.com/live/2021/11/03/world/covid-delta-variant-vaccine#colorado-hospitals**
GIST	Colorado is experiencing its worst coronavirus wave in a year and its overwhelmed hospitals are now allowed to turn away new patients. An executive order, signed on Sunday by Gov. Jared Polis, allowed hospitals to redirect incoming patients. Many medical facilities have reported being over 90 percent capacity, with severe staffing shortages. Covid hospitalizations in Colorado have increased 14 percent in the last two weeks. The state's new daily cases have also increased 14 percent in two weeks, and recently reached their highest level since their peak in November 2020, according to a New York Times database. Hospitals in Larimer County, where vaccine hesitancy is fueling a surge, are using 110 percent of their I.C.U. beds, according to the local health department. That has forced some patients to double up in rooms, and hospitals in the area are close to turning patients away to prioritize emergencies, Tom Gonzales, public health director for Larimer, told CBS Denver. At least 62 percent of the state is fully vaccinated, above the national average of 58 percent. Most hospitalized Covid patients are unvaccinated. At UCHealth, one of the state's biggest health systems, 76 percent of patients hospitalized with Covid-19 are unvaccinated, and over 86 percent of Covid-19 patients who are in need of a ventilator and are in intensive care are unvaccinated.Masks in the state are optional and restaurants are mostly running at full capacity; Mr. Polis, the governor, is reluctant to revive statewide restrictions. The governor's executive order coincided with a state mandate that required health care workers to be fully vaccinated against Covid by Oct. 31. More than 90 percent of Colorado's hospital workers have now been fully vaccinated, according to the state's health department. Last month, the Centers for Disease Control and Prevention urged residents of high-transmission areas to wear masks in public indoor spaces, regardless of their vaccination status, citing evidence that vaccinated Americans with breakthrough infections can carry as much coronavirus as unvaccinated people do. Other nearby states, like Arizona, are also enduring surges. New daily cases are rising faster in Arizona than any other state, up 50 percent over two weeks.
Return to Top	

HEADLINE	**11/03 Air Force hits vaccine deadline: 97% vax**
SOURCE	**https://www.nytimes.com/live/2021/11/03/world/covid-delta-variant-vaccine#air-force-reaches-vaccine-deadline**
GIST	Almost 97 percent of active-duty members of the Air Force — the first branch of the U.S. military to reach its deadline for coronavirus vaccinations — have received at least one dose of vaccine, military officials said Wednesday. That percentage is in line with those for active-duty military members in most branches of service whose deadlines have not yet arrived. Though the 10,636 Air Force members who remain unvaccinated are only a small sliver of the branch's 326,855 active-duty troops, they still represent a large number of people to be facing possible expulsion for failing to comply with the vaccine mandate the Pentagon issued in August.

Many of them have requests pending for an exemption of some kind.

Some 4,933 troops have sought a religious exemption, but so far, not a single member of the military has been granted one. A smaller number have been given an administrative exemption — for example, because they are planning to leave the military soon — and others have received medical exemptions, some of which could be reversed if their medical condition changed. The Air Force said it would take 30 days to review all pending exemption requests.

For the military as a whole, about 97 percent of active-duty forces have had at least one dose of vaccine, and nearly 88 percent are fully vaccinated. The Navy leads the charge, with nearly 99 percent having at least one dose. When the National Guard and Reserves are included as well, though, they drag down the figures considerably, with only 69 percent of all forces fully vaccinated. In the Marines, for example, 86 percent of active-duty troops are fully vaccinated, but only 52 percent of Reserve troops are.

The vaccination deadline for the Navy and Marines arrives later this month. The Army, the largest service branch, has set a date in mid-December. Members of the Guard and Reserves in all branches will also be given more time. Civilian Pentagon employees are required to be fully vaccinated by Nov. 22.

Refusing the vaccine without an exemption is grounds for expulsion from the military, but Defense Secretary Lloyd J. Austin III has given commanders wide latitude to decide how to coax, cajole and ultimately punish those who won't get shots.

"Each case is going to be treated specifically and individually, as it ought to be," John Kirby, a spokesman for Mr. Austin, said this week. "Can we promise you that there will be absolute uniformity across the board? No."

Vaccine reluctance in the military and the Department of Veterans Affairs mirrors that in civilian society, where vaccination rates are generally lower among people who do not face a strict vaccine mandate.

Return to Top

HEADLINE	**11/03 Recall: Tastykake cupcakes**
SOURCE	**https://www.cbsnews.com/news/tastykake-recall-cupcakes-metal/**
GIST	Tastykake cupcakes sold in more than half a dozen states are being recalled because they may contain tiny fragments of metal mesh wire, according to a notice posted by the Food and Drug Administration. Sold by retailers including Target and more than 500 Walmart stores, the multi-pack treats were distributed in Delaware; Maryland; New Jersey; New York; Pennsylvania; Virginia; Washington, D.C.; and West Virginia, according to Thomasville, Georgia-based Flowers Foods, the maker of Tastykakes and one of the biggest U.S. producers of packaged bakery foods. Flowers Foods initiated the recall after being notified by a vendor of the possible contamination in an ingredient. No injuries have been reported. People should not eat the recalled cupcakes but should instead discard them or return their purchase for a refund. Those with questions can call the company at 1(866) 245-8921 during business hours. The following products are being recalled: • Tastykake chocolate cupcakes with the UPC code 0-25600-00219-3 and "enjoy-by" dates of December 14, December 18 and December 21. • Tastykake creme-filled chocolate cupcakes with the UPC code 0-25600-00223-0 and enjoy-by dates of December 14 and December 18.

	• Tastykake buttercreme iced creme filled chocolate cupcakes with the UPC code 0-25600-00230-8 and enjoy-by dates of December 14 and December 18. • Two-count, individually sold packages with the UPC code 0-25600-00004-5 and an enjoy-by date of December 18.
Return to Top	

HEADLINE	**11/03 Nursing school applications increase**
SOURCE	**https://www.cbsnews.com/news/nursing-school-applications-increase-covid-19-burnout/**
GIST	Aspiring nurses are lining up even as the coronavirus pandemic has taken a toll on medical staff. Enrollment in nursing programs across the U.S. increased nearly 6% in 2020 from the year before, according to the American Association of Colleges of Nursing. Nursing school applications at Temple University in Pennsylvania increased about 15% this fall, according to assistant dean Michael Usino. In 2019, almost 7,500 people applied for about 110 spots. Usino said he initially expected the pandemic to reduce interest in nursing. "What we were initially afraid of was that students were going to be seeing the news in social media and what's happening in the hospitals and on the front lines and be dissuaded from nursing," Usino said. "But I think we've been very lucky with this generation of students feeling that inspiration to actually want to serve the community." Leilani Christina Clark said she wants to be a nurse so that she "can make a difference" in someone's life or make their day better "when they're going through a difficult time." Emily Greene said the pandemic has inspired her to pursue a job in health care. "I think with the pandemic, people shy away from health care now, but watching my friends and family work tirelessly, I've never felt more motivated and more excited to be in health care," she said. However, Greene said she was warned about potential burnout. "Burnout is like the first thing that everyone mentions to me like, 'Oh, you're crazy,'" she said. Nursing department chair Mary Terhaar said Temple University makes self-care, mental health and learning how to avoid burnout part of its curriculum. "You think that it's the sciences that you need to master our anatomy and physiology or pharmacology, but you also really need to learn, how do I take care of myself?" Terhaar said.
Return to Top	

HEADLINE	**11/03 Ukrainians protest against vaccination**
SOURCE	**https://abcnews.go.com/Health/wireStory/ukrainians-protest-vaccination-covid-cases-soar-80948558**
GIST	KYIV, Ukraine -- More than a thousand people blocked several streets in the center of the Ukrainian capital Wednesday, protesting against COVID-19 vaccine certificates and state-imposed restrictions aimed at halting the spread of the coronavirus. The protesters, mostly women and young people, didn't wear masks and held up signs reading "Say No to COVID Passports", "Say No to COVID Genocide" in front of the Ukrainian parliament building in Kyiv. The rally comes in response to restrictions that require teachers, government employees and other workers to get fully vaccinated by Nov. 8 or have their salaries suspended. Last week, Ukrainian authorities also started requiring proof of vaccination or negative COVID-19 test results for people boarding airplanes, trains and long-distance buses.

	The measures come as Ukraine reports a record-high level of new infections and deaths from the coronavirus. Authorities have mainly blamed the surge on widespread public reluctance to get vaccinated. Ukrainians can freely choose between the Pfizer-BioNTech, Moderna, AstraZeneca and Sinovac vaccines, but just about 17.1% of the 41-million population has been fully vaccinated, which is Europe's second-lowest rate after Armenia. "I don't want to participate in an experiment on myself, but I am deprived of the right to choose," said Tamara Ustinova, 35, a teacher from Mariupol. "The authorities force Ukrainians to get vaccinated, creating unbearable conditions, but the danger of genetic mutations is much greater than the harm from COVID." The police did not interfere with the rally, which was supported by ex-lawmaker Nadiya Savchenko who was detained at an airport a few weeks ago with a fake vaccination certificate. "The authorities will only aggravate the situation further," Savchenko said at the rally. "You have the right to move freely around the country, this is everyone's right." Savchenko and the protesters held several prayers in front of the parliament building. The government says that some denominations oppose vaccination, and false rumors about vaccines containing microchips, causing gene mutations or infertility are circulating among believers. New government regulations and restrictions have spawned a booming black market for counterfeit documents. Fake vaccination certificates are selling for the equivalent of $100-300, and there have been reports of a fake version of a government digital app with fake certificates already installed. Authorities have opened 1,065 criminal cases over the distribution of fake certificates involving 80 doctors and 35 travel agencies. Police have blocked 40 websites that offered fake certificates. Parliament has proposed to make the use and production of fake certificates a separate criminal offence, punishable by up to three years in prison or a fine of about $6,460. A bill to that effect has already been supported by lawmakers in the first reading on Tuesday. "The anti-vaccination spirit quickly disappears in intensive care, and fake certificates do not work there," Health Minister Viktor Lyashko said at a briefing. "Calls not to get vaccinated are, in my opinion, a mockery of our doctors and families who have lost their relatives." In total, Ukraine has reported 2,979,086 coronavirus cases and 69,447 deaths.
Return to Top	

HEADLINE	**11/03 UK official: hard months ahead Covid rates**
SOURCE	**https://abcnews.go.com/Health/wireStory/uk-official-warns-hard-months-ahead-amid-high-80946155**
GIST	LONDON -- England's deputy chief medical officer said Wednesday that too many people believe the pandemic is over, warning that the U.K.'s very high coronavirus rates and rising deaths mean that there are "hard months to come in the winter." Jonathan Van-Tam also said he was worried that increasing numbers of deaths showed infections were "now starting to penetrate into older age groups." Coronavirus "rates are still very high at the moment. They are higher than in most of Europe," Van-Tam told the BBC. "We are running quite hot. And, of course, it's of concern to scientists that we are running this hot this early in the autumn season."

	"I personally feel there are some hard months to come in the winter and it's not over," he added. The British government reported 41,299 new COVID-19 cases and 217 deaths Wednesday. The country recorded its highest daily death toll since February - 293 - on Tuesday. While new cases have been dropping from around 46,000 a day in October, infection rates in Britain are still much higher than in most of Europe. Van-Tam said the drop in case numbers mainly reflected the ebbing of a surge recently seen among teenagers. He warned that while hospital admissions have plateaued and total numbers of patients in hospitals have slightly gone down, the overall picture was still worrying. "This could be a pause before things go up, it could be the very first signs that things are beginning to stabilize but at a high rate," he said. "But my worry is that the deaths are increasing and that shows that the infection is now starting to penetrate into those older age groups." The U.K. got a head-start in rolling out its vaccination program, and most adults have been fully inoculated. A booster shot is being offered to millions, including everyone over 50. But the government has been cautious about vaccinating teenagers and younger people, authorizing jabs for healthy children between 12 to 15 years old only this September. Jeremy Brown, a member of the government's vaccination advisory committee, said it was "far too early" to follow the lead of the United States in vaccinating children 11 years old and under. Prime Minister Boris Johnson's Conservative government lifted almost all coronavirus restrictions in July, including mandatory face coverings and social distancing requirements. Nightclubs and crowded venues were allowed to fully open and the work from home advice was scrapped. Authorities have resisted calls to reimpose restrictions like mandatory mask-wearing, and are instead relying heavily on vaccines to keep infections down.
Return to Top	

HEADLINE	**11/03 Europe Covid cases rise 5th straight week**
SOURCE	**https://abcnews.go.com/Health/wireStory/covid-19-cases-rise-europe-5th-consecutive-week-80943924**
GIST	GENEVA -- The number of coronavirus cases has risen in Europe for the fifth consecutive week, making it the only world region where COVID-19 is still increasing, the World Health Organization reported Wednesday. In its weekly report on the pandemic, the U.N. health agency said new cases jumped by 6% in Europe compared to an 18% increase the previous week. The weekly number of new infections in other regions either fell or remained about the same, according to the report. The sharpest drops were seen in the Middle East, where new cases decreased by 12%, and in Southeast Asia and Africa, where they fell by 9%. Overall, 3 million new weekly cases were reported globally, the report states. The number of deaths from COVID-19 worldwide rose by 8%, driven mainly by Southeast Asia, where deaths spiked by 50%. The coronavirus infection rate was by far the highest in Europe, which reported about 192 new cases per 100,000 people, followed by the Americas, which had about 72 new cases per 100,000. Several countries in Central and Eastern Europe have seen daily case numbers shoot up in recent weeks. Infections in the Czech Republic soared by 9,902 in one day, the Czech Health Ministry reported Wednesday. That was about 60% more than a week earlier and the highest daily increase since March 23, the ministry said.

	The country had a 7-day infection rate of 386 people per 100,000, almost double the figure from a week ago. The government has said the virus is spreading mostly among people who are unvaccinated. Poland's Health Ministry on Wednesday reported the country's highest daily number of new cases since April, with over 10,400, or 20% more than a week earlier. The ministry said more than 120 people with COVID-19 died over 24 hours. In Germany, the head of the national disease control center said that infection rates have risen "rapidly," with significantly more patients in intensive care and deaths rising above 100 per day on some recent occasions. "Unfortunately, the fourth wave is developing exactly as we had feared, because not enough people are vaccinated and because measures … are no longer being implemented sufficiently," Robert Koch Institute President Lothar Wieler said in Berlin. He cited measures such as mask-wearing and distancing, and restrictions on people who haven't been vaccinated or tested using some facilities. Wieler's Robert Koch Institute reported 20,398 new cases over the past 24 hours, putting the rate of new infections at 146.6 per 100,000 residents over the past week. Another 194 deaths were reported, pushing Germany's total so far above 96,000. WHO said the continuing rise in confirmed cases across Europe has been driven mostly by Britain, Russia, Turkey and Romania, the report showed. Leading British medical authorities have called for the government to again require infection precautions such as mask-wearing and social distancing, but the government has insisted the health system can handle the increasing caseload. Some scientists worry that waning immunity from vaccinations across Europe could allow even more people to fall ill from COVID-19 during the winter season. WHO nevertheless has slammed rich countries for rolling out booster vaccine programs while the majority of poor countries have yet to administer shots to their most vulnerable populations; the agency said last week that about 1 million booster shots are administered every day, about three times the number of COVID-19 doses given in poor countries. WHO said the easier-to-spread delta variant remains predominant worldwide and continues to mostly crowd out other variants; more than 99% of COVID-19 samples sequenced by an international database were the delta variant. It said delta's spread has been slightly slower in some parts of South America, where other variants, including the mu variant, account for a large proportion of cases.
Return to Top	

HEADLINE	**11/03 Russia Covid surge shows no signs abating**
SOURCE	**https://abcnews.go.com/Health/wireStory/russia-covid-19-surge-shows-signs-abating-80944850**
GIST	MOSCOW -- Daily coronavirus cases and deaths in Russia remained at their highest numbers of the pandemic Wednesday as more regions announced they were extending existing restrictions in an effort to tame the country's unrelenting surge of infections. Russia's state coronavirus task force reported 40,443 new confirmed cases from a day earlier. It was the fifth time in seven days that the country reported more than 40,000 infections. The task force also reported a daily record of 1,189 COVID-19 deaths.

Russia is five days into a nationwide non-working period that the government introduced to curb the spread of the virus. Last month, Russian President Vladimir Putin ordered many Russians to stay off work between Oct. 30 and Nov. 7. He authorized regional governments to extend the number of non-working days, if necessary.

Officials in Russia's Novgorod region, located 500 kilometers (310 miles) northwest of Moscow, said Monday that the time away from workplaces would last another week. Four other regions — the Tomsk region in Siberia, the Chelyabinsk region in the Ural Mountains, the Kursk and the Bryansk regions southwest of Moscow — followed suit Wednesday. The Smolensk region on the border with Belarus also extended the non-working days, but only until Nov. 10.

“One non-working week is not enough to break the chain of infection,” Tomsk governor Sergei Zhvachkin said.

Governors of at least three other regions have said they were considering extending the non-working period.

Kremlin spokesman Dmitry Peskov said Wednesday that no decision on a possible nationwide extension has been made.

“If any other decisions are (made), we will inform you,” Peskov said during a conference call with reporters.

In Moscow and the surrounding region, which together account for nearly 25% of new daily infections, the non-working period will not be extended beyond Nov. 7, officials said.

Moscow Mayor Sergei Sobyanin said infection rates in the capital have “stabilized," and the governor of the Moscow region, Andrei Vorobyov, echoed his sentiment.

Certain restrictions will remain in place in the Russian capital, such as a stay-at-home order for older adults and a mandate for businesses to have 30% of their staffs work from home. Access to theaters and museums is limited to those who either have been fully vaccinated, have recovered from COVID-19 within the last six months or can present a negative coronavirus test.

Russia’s weekslong surge in infections and deaths comes amid low vaccination rates, lax public attitudes toward taking precautions and the government’s reluctance to toughen restrictions.

Less than 35% of Russia’s nearly 146 million people have been fully vaccinated against the coronavirus, even though Russia approved a domestically developed vaccine against the coronavirus months before most countries.

In all, Russia’s state coronavirus task force has reported more than 8.6 million confirmed coronavirus cases and over 242,000 deaths in the pandemic — by far the highest death toll in Europe.

However, reports by Russia’s state statistical service Rosstat that tally coronavirus-linked deaths retroactively reveal much higher mortality numbers. A report released last week indicated that some 462,000 people with COVID-19 died between April 2020 and September of this year.

Russian officials have said the task force only includes deaths for which COVID-19 was the main cause and uses data collected from medical facilities. Rosstat uses wider criteria for counting virus-related deaths and takes its numbers from civil registry offices where the process of registering a death is finalized.

Return to Top

HEADLINE	**11/04 India celebrates Hindu festival of lights**
SOURCE	**https://abcnews.go.com/International/wireStory/indians-celebrate-festival-light-amid-covid-19-fears-80965324**

GIST	NEW DELHI -- Indians across the country began celebrating Diwali, the Hindu festival of lights, on Thursday amid concerns over the coronavirus pandemic and rising air pollution. Diwali is typically celebrated by socializing and exchanging gifts with family and friends. Many light oil lamps or candles to symbolize a victory of light over darkness, and fireworks are set off as part of the celebrations. Last year, celebrations in India were upended by a renewed spike in COVID-19 infections, but festivities this year seem to be back. Even though the government has asked people to avoid large gatherings, markets have been buzzing ahead of Diwali, with eager crowds buying flowers, lanterns and candles. As dusk fell on Wednesday, over 900,000 earthen lamps were lit and kept burning for 45 minutes in the northern city of Ayodhya in Uttar Pradesh state, retaining the Guinness World Record it set last year. As part of the Diwali celebrations, the city last year lit 606,569 oil lamps. The lamps were lit at Ram ki Pauri, at the banks of Saryu River, a stunning spectacle for thousands of visitors who thronged its shores while ignoring coronavirus social distancing norms. A laser and fireworks show followed, illuminating the city's lanes and river banks. Thousands of city residents also lit lamps at their houses and temples. The festival is being celebrated at a time when India's pandemic crisis has largely subsided. On Thursday, the country recorded over 12,000 new coronavirus cases and 461 deaths, a far cry from earlier this year when India buckled under a few hundred thousand new infections every day. Overall, it has recorded more than 35 million infections and over 459,000 deaths, according to the Health Ministry. These figures, as elsewhere, are likely undercounts. Even states where infections were swelling a few weeks ago, such as Kerala along the tropical Malabar Coast, have seen a sustained decline. India also celebrated administering its billionth COVID-19 vaccine dose last month, further boosting confidence that life is returning to normal. Still, experts have warned that the festival season could bring a renewed spike in infections if COVID-19 health measures aren't enforced. There are also worries over air pollution, which typically shrouds northern India under a toxic grey smog at this time as temperatures dip and winter settles in. On Diwali night, people also lit up the sky with firecrackers — their smoke causing pollution that takes days to clear. While there is no nationwide ban on bursting firecrackers, a number of states have imposed restrictions to stem the pollution, with some allowing their residents to light green crackers for a certain number of hours. Green crackers produce lesser emissions than normal firecrackers. In the past, similar bans have often been flouted.
Return to Top	

HEADLINE	**11/03 China advice spark speculation Taiwan war**
SOURCE	**https://abcnews.go.com/International/wireStory/chinas-advice-stockpile-sparks-speculation-taiwan-war-80965524**
GIST	BEIJING -- A seemingly innocuous government recommendation for Chinese people to store necessities for an emergency quickly sparked scattered instances of panic-buying and online speculation: Is China going to war with Taiwan? The answer is probably not — most analysts think military hostilities are not imminent — but the posts on social media show the possibility is on people's minds and drew out a flurry of war-mongering comments.

Taiwan is a self-governing island of 24 million people China regards as a renegade province that should come under its rule. Tensions have risen sharply recently, with China sending a growing number of warplanes on sorties near the island and the U.S. selling arms to Taiwan and deepening its ties with the government.

Most residents interviewed in Beijing, the Chinese capital, thought war was unlikely but acknowledged the rising tensions. They generally favored bringing Taiwan under Chinese rule by peaceful means, the official position of China's long-ruling Communist Party.

“I don’t feel panic but I think we should be more alert about this than in the past,” said Hu Chunmei, who was taking a neighborhood walk.

War fears or not, there were scattered reports of runs on rice, noodles and cooking oil in some Chinese cities, according to local media. The more immediate worry for some was the possibility of neighborhood lockdowns as a COVID-19 outbreak spreads in several provinces.

The government moved quickly to try to tamp down fears with assurances of sufficient supplies. A bright yellow sign in an aisle of a Beijing supermarket asked customers to buy reasonably and not to listen to rumors or stockpile goods.

The online speculation started with a Commerce Ministry notice posted Monday evening about a plan to ensure the supply and stable price of vegetables and other necessities for the winter and spring. A line in it encouraged families to store some necessities for daily life and emergencies.

That was enough to set off some hoarding and a discussion on social media that the ministry could be signaling people should stock up for war.

China's state media has covered the rising tensions with Taiwan heavily, including the often-tough words exchanged between China on one side and the U.S. and Taiwan on the other.

“It is natural to have aroused some imagination,” social commentator Shi Shusi said. “We should believe the government’s explanations, but the underlying anxiety deserves our thought.”

He said the populist views cheerleading for war don't represent majority opinion but do send a signal or warning to Taiwan.

Other developments fueled the war speculation. One person shared a screenshot of a list of recommended emergency equipment for families issued in August by the government in Xiamen, a coastal city near an outlying Taiwanese island. An unverified report — denied Wednesday by a military-affiliated social media account — said veterans were being called back to service to prepare for combat.

It's difficult to gauge how many people interpreted the notice as a possible prelude to war, but the reaction was strong enough to prompt a state media response the next day.

The Economic Daily, a government-owned newspaper, said people's imagination shouldn't run so wild, explaining that the advice was meant for people who may find themselves suddenly locked down because of a COVID-19 outbreak.

Hu Xijin, the editor-in-chief of the Global Times newspaper, blamed the the online speculation on the amplification of public opinion during a time of tension.

“I do not believe that the country wants to send a signal to the public at this time through a notice from the Commerce Ministry that people need to ‘hurry up and prepare for war,’" he wrote.

	Zhang Xi, another Beijing resident, ruled out the possibility of war and counseled patience in a dispute extending to when Taiwan and China split during the civil war that brought Mao Zedong's Communists to power in 1949. “This is a leftover from history, and it’s impossible to solve this right away," she said.
Return to Top	

HEADLINE	**11/03 Maldives faces dire climate change threat**
SOURCE	**https://abcnews.go.com/International/facing-dire-sea-level-rise-threat-maldives-turns/story?id=80929487**
GIST	The Maldives are well known as a bucket list getaway. Hearing the country's name conjures up images of luxury huts overlooking an aqua blue ocean. But climate change may cross the country off the map completely. The archipelago, which is made up of over 1,100 coral islands in the middle of the Indian Ocean, is the lowest lying nation in the world. Therefore, sea level rise caused by global climate change is an existential threat to the island nation. At the current rate of global warming, almost 80% of the Maldives could become uninhabitable by 2050, according to multiple reports from NASA and the U.S. Geological Survey. "Our islands are slowly being inundated by the sea, one by one," Ibrahim Mohamed Solih, the president of the Maldives, told the U.N. Climate Change Conference, or COP26, earlier this week. "If we do not reverse this trend, the Maldives will cease to exist by the end of this century." The islands that are home to local Maldivians, not the resort islands, stand to lose the most. Mohammed Nasheed, the former president of the Maldives and a leading voice for climate change equity, told ABC News that more than 90% of islands in the Maldives have severe erosion, and 97% of the country no longer has fresh groundwater. Ibrahim Mubbasir and his family live on the island of Dhiffushi. It is suffering from severe erosion, and flooding has increased from two or three times a year to twice a month. Four years ago, the family's well became unusable because of salt water contamination, leaving them to rely on collecting rainwater. Mubbasir said they only have enough fresh water to last for three more months. "Things that we thought would happen towards the end of the century, we are experiencing now," Aminath Shauna, the Maldives' minister of environment, climate change and technology, told ABC News' Ginger Zee. Shauna said that more than 50% of the national budget is spent on adapting to climate change. When asked what the Maldives will look like in 2050, Shauna responded, "Are you willing to take the Maldives as climate refugees? I think that's the conversation that needs to happen." And it's not just the Maldives. Island countries around the world have been asking developed nations for funds since 2009. Countries with the highest greenhouse gas emissions -- China, the United States and India -- are mostly responsible for the rapid sea level rise. At the center of the Maldives' culture are their coral reefs. In 2016, the Maldives lost their front line of defense when a bleaching event affected about 60% of the coral reefs, according to Aya Naseem, a marine biologist and co-founder of the Maldives Coral Institute. Without coral reefs, the islands are wide open to the rising waters. Naseem said they have one realistic choice: They need to build back and protect the reefs, "because IPCC (Intergovernmental Panel on Climate Change) is predicting that by 2050 if the temperature rises 1.5 degrees Celsius we can lose 70 to 90% of corals in the whole world."

	Research has previously shown that a healthy coral reef can absorb 97% of wave energy, dramatically reducing erosion, and it's affordable, Naseem said. "It's much cheaper than building a seawall. I think it costs something like $3,000 to grow a meter of sea wall where for the coral a meter of it is about $300, including monitoring and everything," she said. Bebe Ahmed, founder of "Save the Beach," travels island to island in the Maldives with the mission of teaching kids about restoring and protecting coral. He told ABC News that his dream is to inspire young Maldivians to want to start their own projects to restore coral reefs. What's next in the fight? Technology, like 3D-printed coral structures or a floating city, may have to be part of the solution. The Maldives is home to the Modular Artificial Reef Structure, or MARS, a coral-forming project on the resort island of Summer Island. to the coral forming project, MARS. The project has 3D-printed bases that are placed in the water with transplant corals attached to them. The hope is that the system is designed with the specific needs of the coral farm in mind, providing a permanent structure for coral to grow. In the late '90s, the Maldives began construction on the island of Hulhumale through the process of land reclamation. Hulhumale is 6.5 feet above sea level, more than double the height of Male, the current capital of the Maldives. It is possible this island may be a future site for relocation of Maldivians suffering from sea level rise. Maldivians call their manmade island the City of Hope. The future of the Maldives could also come in the form of a floating city. In 2022, just a few miles from the dense, capital city of Male, construction and assembly will begin on the world's first true floating city. The unique solution will not have to worry about sea level rise, because it will always be on top of the sea. The project is being developed and led by Dutch Docklands in the Netherlands. Lead architect Koen Olthuis gave ABC News an inside look at how the floating city is designed and what it should eventually look like. The floating city has a unique pattern, modeled after the brain, both human and coral. The entire city will shift up and down on a pile drilled into the sea floor. It will also take advantage of its environment to better provide for those living on the floating city. "By being on the water we want to take advantage of the water -- and using the coolness of the water -- so these are water-cooled cities, for which you take cool water outside the atoll and pump water through the route and activate the air conditioning systems," Olthius said. Since the floating city is sustainable and leaves no footprint, Olthuis called the floating cities "scarless" and said they are "renting space from nature."
Return to Top	

HEADLINE	**11/03 Men behind vast majority of gun violence**
SOURCE	**https://abcnews.go.com/US/guys-guns-men-vast-majority-americas-gun-violence/story?id=79125485**
GIST	Just before 11 p.m. on an April night, a 19-year-old man arrived at his former job site, an Indianapolis FedEx facility, and chatted with security about his status at the company. The young man then exited his car with two legally purchased rifles and opened fire indiscriminately, at employees inside and outside the building, authorities said. After killing eight employees -- ranging in age from 19 to 74 -- and injuring at least seven others, the gunman died by suicide, an attack "which he believed would demonstrate his masculinity and capability of

fulfilling a final desire to experience killing people," the FBI in Indianapolis said this summer, months after the attack.

According to the nonprofit research center The Violence Project, men are responsible for 98% of mass shootings, and according to an analysis by Everytown for Gun Safety, a grassroots organization aiming to combat gun violence, men were behind 94% of 240 mass shootings (four or more killed regardless of location) from 2009 to 2020 in which the shooter's gender could be confirmed.

In 40 active-shooter incidents in the U.S. last year, 35 shooters were male, three were female and four were unspecified, according to FBI data.

The gender gap goes beyond active shooter incidents. Of 16,245 murders in the U.S. in 2019, in those for which a suspect's gender was identified, 10,335 (63%) were committed by men, according to FBI data. Gun violence victims also are predominantly male, accounting for 85% of fatalities and 87% of injuries through May, according to the Centers for Disease Control and Prevention.

But women are also deeply affected by gun violence, often as grieving family members or because they're left as sole caregivers of children in the wake of the violence.

Or as victims themselves.

So why are American men so much more prone to gun violence? Experts cite a variety of reasons, from brain chemistry and evolution to how men and boys are socialized, said Jillian Peterson, co-founder of The Violence Project and a professor of criminology and criminal justice at Hamline University.

But other experts said it really just comes down to what they say is arguably America's most dangerous combination: toxic masculinity and gun availability.

'Only America'

Shannon Watts, founder of Moms Demand Action, said toxic masculinity, the cultural idea that manhood is defined by violence and aggression to maintain power or strength, is at the root of both domestic violence and mass shootings, adding that there's one reason gun violence is a "uniquely American issue" -- it's easy to get guns.

Men commit about 90% of murders worldwide (including but not limited to the use of firearms), according to a 2019 United Nations report. But America's gun homicide rate is 25 times higher than other high-income countries, according to Everytown for Gun Safety.

"Every country has racism, xenophobia, hatred. Only America gives those same people" access to guns, Watts said.

Gender studies expert Michael Kimmel agreed.

The traditional idea of masculinity is, "You don't get mad, you get even," Kimmel said. "The capacity for violence has been a hallmark of masculinity since the beginning of writing. Go back to 'The Iliad.' The Bible is filled with stories about vengeful violence."

"That is true for masculinity in other countries, in other cultures," Kimmel said. "So you have to also ask yourself: Why is it that gun violence at the scale that we see it is a phenomenon" in the U.S.?

"You have to ask the question," Kimmel continued, 'Why here and not elsewhere?' The ideology of masculinity is not all that different in Spain or Britain than it is here. But they don't have mass shootings like this. Why? I think that has to do with a specific version of American masculinity."

Kimmel said American men are responsible for such a staggering sum of shootings because of that ideological masculinity, American culture, which he said gives a "constant presentation of enemies," real or imagined, and -- the most significant contributor -- easy access to guns.

The power of 'protection'
Kimmel says protection also plays an important role.

"If you ask American men, what's the role of a man? He will tell you, 'To provide for and protect my family,'" Kimmel said. "In this uncertain economic world, being a provider is actually far more difficult than it was in my father's generation, than it was in his father's generation. I think some part of American men's fascination with guns and arming themselves has to do with, 'If I can't be a provider, at least I can be a protector.'"

About 45% of American men last year said they owned a gun, according to Gallup, and 19% of American women said they did.

In a 2017 Pew Research Center poll, 67% of gun owners said protection was a major reason for ownership, Iowa State professor Craig Rood noted in a Gender Policy Report through the University of Minnesota. Protection was followed by: hunting, sport shooting, as part of a collection and for one's job.

Only 26% mentioned protection in a 1999 Pew Research Center poll in which hunting ranked No. 1, Rood noted.

"I could imagine several explanations why Americans are more afraid today than they were in 1999," Rood told ABC News. "For instance, gun sales spiked after several high-profile mass shootings and again when the COVID-19 pandemic began. But not everyone has responded to that fear by turning to guns."

"When we are talking about 'protection,' we are talking about perception of danger, and perceptions of danger can be real, imagined or some place in between," Rood said. "Statistically, the United States has been relatively safe for most people, as crime and homicide rates started falling from the mid-1990s until quite recently. Yet the perception of danger has increased. So, there's an obvious mismatch."

Rood added, "I would bet most men acquire guns for commendable reasons: They want to protect themselves or their family, they enjoy hunting or they simply like guns. But the very presence of a gun in the home opens the possibility for accidents. Guns also heighten the risk for completed suicide and deadly intimate-partner violence."

What can be done?
Peterson, of the Violence Project, said the key to fewer shootings is prevention, and offered four prongs.

1. Prevention should start early, by teaching boys how to understand emotions and trauma.

"Think about things like trauma screening and teaching social and emotional learning in schools ... teach young boys how to cope with emotions and have empathy," she said.

When it comes to male mass shooters, Peterson said many tend to have an attitude that "the world owes me more than what I have."

"They feel disappointed where they're at in life, or they feel frustrated that they lost their job or that they can't get a girlfriend or whatever it is ... so they pick a target of who to blame, whether they pick women or their school or a racial group," Peterson said.

In July, a 21-year-old Ohio man was charged for allegedly trying to carry out a mass shooting of women, prosecutors said. He allegedly compared his "extremely empowering action" to Elliot Rodger, a 22-year-old man who carried out a mass shooting at the University of California, Santa Barbara in 2014 after videotaping his rage over his rejection by women and vowed "retribution." The Ohio 21-year-old

allegedly had a manifesto, according to prosecutors, in which he wrote he "would 'slaughter' women 'out of hatred, jealousy and revenge.'"

2. Peterson said the U.S. also needs better systems for crisis training and how to recognize and report someone's potential crisis.

According to The Violence Project, 82% of men who commit shootings are suffering from a noticeable crisis, with most showing at least one of the following symptoms and more than one-third exhibiting five or more: increased agitation, abusive behavior, isolation, losing touch with reality, depression, mood swings, paranoia and an inability to complete daily tasks.

Peterson said she considers the lack of a social safety net, which impacts trauma and crisis, to be a uniquely American problem.

3. Potential mass shooters often look online for others who validate their thoughts and feelings, or research past or potential shooters, Peterson said, so internet companies, especially social media platforms, must be pressured to better regulate hateful rhetoric and content.

Watts said parents also have a part in this.

"Every nation is home to young men being radicalized online to believe that somehow a loss of power means that they need to become violent," Watts said.

Watts said she's constantly talking to her 20-year-old son about how the internet is home to platforms "where this kind of violent rhetoric can become ingrained."

"It's a conversation that all parents need to have, in particular with their sons," she added.

4. Peterson said another uniquely American problem is the struggle to regulate access to guns, like through red flag laws, which allow the court to remove an individual's guns for a certain amount of time if a judge finds he or she is a danger.

Watts stressed the need for more background checks, noting that only 21 states and Washington, D.C., require background checks on all gun sales -- meaning that in every other state, someone looking to acquire a gun quickly can do so at a gun show or via a private transaction.

Watts is also pushing for substantive legislative change, including advocating for an update to the Violence Against Women Act that would include a provision that would prevent abusive dating partners or alleged stalkers from accessing a gun.

The current law doesn't define abusive dating partners or alleged stalkers as domestic abusers, and instead focuses on spouses and live-in partners, which Watts called a loophole.

Every 16 hours a woman in America is shot dead by a current or former partner, according to the Brady Campaign to Prevent Gun Violence. Further, an Everytown analysis found that in at least 53% of American mass shootings from 2009 to 2020, the gunman also shot a current or former intimate partner or family member.

The VAWA, initially passed in 1994 and expanded in later years, has since expired.

"It's really toxic masculinity that's at the root of domestic violence and mass shootings -- misogyny and easy access to guns," Watts said. "Guns are the weapons of choice for extremists, for misogynists, for insurrectionists and, ultimately, women are paying the price with their lives."

Return to Top

HEADLINE	**11/03 Minneapolis vote on police reform**

SOURCE	https://abcnews.go.com/US/minneapolis-vote-police-reform-means-movement/story?id=80946157
GIST	Minneapolis voters on Tuesday rejected a charter amendment that would have replaced the Minneapolis Police Department with a Department of Public Safety. About 56% of voters voted "no" on the charter amendment, which was pitched as a "public health approach" to policing in response to the anti-police brutality movement of 2020. Corenia Smith, campaign manager for Yes 4 Minneapolis, the group behind the charter proposal, released a statement on the proposal's loss. "This campaign began with working-class Black and brown residents marching together to demand a higher standard of public safety in the city," Smith said. "It grew into a citywide movement that spanned race, income and neighborhoods, to give residents a say in their future and to advocate for the resources that they need." The amendment would have removed the police department from the city's charter, removed the requirement to employ 1.7 officers for every 1,000 residents and would have replaced the police chief with a commissioner, who would be nominated by the mayor and approved by the city council. Police reform has been a powder keg issue following the death of George Floyd, a Black man who was killed by former Minneapolis police officer Derek Chauvin. His death prompted national divisions over whether to "defund" policing systems across the country in order to change the way departments operate. "While this is not the result that we hoped for, the story of our movement must be told," Smith wrote. Yes 4 Minneapolis collected over 22,000 signatures, knocked on over 100,000 doors, made almost 200,000 phone calls and sent 300,000 text messages to Minneapolis residents about expanding public safety in the city, according to Smith. MORE: Ballot question asks Minneapolis voters to consider replacing police department The movement, which also included the work of partnering organizations, faced several challenges, including a lawsuit by several Minneapolis residents who sued the city council for promoting a "misleading ballot question." Those residents claimed in the lawsuit that the council "approved an incomplete and misleading ballot question regarding an amendment to the City Charter that would eliminate the Minneapolis Police Department without any plan for replacing that department's critical public safety functions." The proposal language was challenged several times and vetoed by Mayor Jacob Frey until the city council finally passed the official language that appeared on the ballot. Frey, a member of the Minnesota Democratic–Farmer–Labor Party, denounced the efforts. "My primary reason for opposing this charter amendment comes down to accountability," Frey previously said in a statement to ABC News. "If passed, this proposal will dilute accountability by diffusing responsibility for public safety across 14 policymakers. The result would likely leave voters -- and the department -- uncertain of who among the 13 council members and mayor’s office is actually directing, and responsible for, the department’s activity." Frey said he believes that a change in department leadership would lead to a major setback for "accountability and good governance." Smith claims the proposal was misrepresented throughout the campaign season by Frey and others who oppose the changes to policing.

	"We spoke the truth, while the opposition, Democrats and Republicans alike, spread lies and mischaracterized our measure to create confusion, distrust and fear," Smith alleged. Some voters also said the charter change was confusing and lacked specifics and a clear message of how the transition would affect the city. "I knew it wasn't gonna pass," said Tallaya Byers, a North Minneapolis resident who was in favor of the amendment. "There's a lot of people that don't understand. It was all confusing. People didn't understand the plan behind replacing it with the Public Safety Department. So I knew that it was going to end up like that." Some voters say a lack of resident input helped lead the proposal to its downfall. "[Voters] want to take an approach that is well thought out, well researched and includes the voices and perspectives of community members who are normally marginalized in our society," said Minneapolis resident Nekima Levy Armstrong, who was against the charter amendment. Teto Wilson, a North Minneapolis resident who was also against the charter amendment, said he rejected the amendment because it seemed "arbitrarily" put together and hopes the council works on a more thorough plan for the city in the upcoming legislative periods. Leili Fatehi, the campaign manager of All of Mpls, an advocacy group against the charter, said she hopes Mayor Jacob Frey and the city council commit to addressing the issues of policing. "Minneapolis voters have made clear that they want a planful approach to transforming policing and public safety in our city that includes meaningful consultation with the communities most impacted by violence and over-policing, and a real conversation about how to ensure every resident is protected from crime and from police brutality," Fatehi said in a statement to ABC News. Despite the loss, activists say that their efforts won't stop, as roughly 43% of people voted "yes" for the charter amendment. "Even though ballot question #2 wasn't approved this year, we will continue to fight to expand what safety looks like for Black and brown communities," Rashad Robinson, the spokesperson for Color of Change, said. "In doing so, we will challenge how our society views safety and the resources attached to addressing public safety, in hopes of providing a more just and equitable future for all."
Return to Top	

Cyber Awareness

Top of page

HEADLINE	**11/04 Justice Dept. cyber crackdown**
SOURCE	**https://apnews.com/article/technology-russia-crime-arrests-hacking-f0adf6f0765b0f079a20a95cf85c5334**
GIST	WASHINGTON (AP) — The Justice Department is stepping up actions to combat ransomware and cybercrime through arrests and other actions, its No. 2 official told The Associated Press, as the Biden administration escalates its response to what it regards as an urgent economic and national security threat. Deputy Attorney General Lisa Monaco said that "in the days and weeks to come, you're going to see more arrests," more seizures of ransom payments to hackers and additional law enforcement operations. "If you come for us, we're going to come for you," Monaco said in an interview with the AP this week. She declined to offer specifics about who in particular might face prosecution. The actions are intended to build off steps taken in recent months, including the recent extradition to the U.S. of a suspected Russian cybercriminal and the seizure in June of $2.3 million in cryptocurrency paid to

hackers. They come as the U.S. continues to endure what Monaco called a “steady drumbeat” of attacks despite President Joe Biden’s admonitions last summer to Russian counterpart Vladimir Putin after a spate of lucrative attacks linked to Russia-based hacking gangs.

“We have not seen a material change in the landscape. Only time will tell as to what Russia may do on this front,” Monaco said.

Another official, National Cyber Director Chris Inglis, painted a rosier picture, telling lawmakers Wednesday that the U.S. had seen a “discernible decrease” in attacks emanating from Russia but that it was too soon to say why.

But Monaco added: “We are not going to stop. We’re going to continue to press forward to hold accountable those who seek to go after our industries, hold their data hostage and threaten economic security, national security and personal security.”

Monaco is a longtime fixture in Washington law enforcement, having served as an adviser to Robert Mueller when he was FBI director and as head of the Justice Department’s national security division. She was a White House official in 2014 when the Justice Department brought a first-of-its-kind indictment against Chinese government hackers.

Monaco’s current position, with oversight of the FBI and other Justice Department components, has made her a key player in U.S. government efforts against ransomware. That fight has defied easy solutions given the sheer volume of high-dollar attacks and the ease with which hackers have penetrated private companies and government agencies alike. How much lasting impact the latest actions will have is also unclear.

Though not a new phenomenon, ransomware attacks — in which hackers lock up and encrypt data and demand often-exorbitant sums to release it to victims — have exploded in the last year with breaches affecting vital infrastructure and global corporations.

Colonial Pipeline, which supplies roughly half the fuel consumed on the East Coast, paid more than $4 million after a May attack that led it to halt operations, though the Justice Department clawed the majority of it back by gaining access to the cryptocurrency wallet of the culprits, known as DarkSide. The public should expect to see more such seizures, Monaco said.

JBS, the world’s largest meat processor, paid $11 million in June following a hack by a Russian group known as REvil, which weeks later carried out what’s believed to be the largest single ransomware attack on record — largely through firms that remotely manage IT infrastructure for multiple customers.

The splashy attacks elevated ransomware as an urgent national security priority while the administration scrambled to stem the onslaught.

Inside the Justice Department, officials in April formed a ransomware task force of prosecutors and agents, and they’ve directed U.S. attorney offices to report ransomware cases to Washington just as they would terrorism attacks.

It has also tried prosecutions, extraditing from South Korea last month an accused Russian hacker, Vladimir Dunaev, who prosecutors say participated in a cyber gang whose malicious software — “Trickbot” — infected millions of computers.

“You’re going to see more actions like you saw last week in the days and weeks to come,” Monaco said.

Still, holding foreign hackers accountable in the U.S. is notoriously difficult, and ransomware gangs are abundant. Even if recent attacks haven’t generated the same publicity as the ones last spring, Monaco said there’s been no discernible change in behavior by opportunistic hackers still targeting a range of industries with attacks that threaten to paralyze crucial business operations — or force multimillion-dollar payouts.

	Monaco said she's sympathetic to the hard decisions companies must make, in part because she's had experience confronting criminals' monetary demands. As homeland security and counterterrorism adviser in the Obama administration, she helped craft a policy on Americans held hostage overseas. The policy reiterated that ransom payments for hostages were discouraged and illegal, but also made clear that prosecutors didn't plan to prosecute families who made such payments. "What it reflects, and frankly what the whole endeavor reflected, was a sense on Lisa's part that this was an area where you needed an extraordinary balance between policy and humanity," said Joshua Geltzer, the Biden administrator's deputy homeland security adviser who worked with Monaco in the Obama White House. The U.S. government has publicly discouraged ransomware payments but Monaco — who during the Obama administration faced criticism from hostage families about the government's response to their plight — says the administration is trying to listen to and work with victimized companies. Officials have shown no interest in prosecuting companies that pay ransom to hackers, though Monaco did announce last month that the department was prepared to sue federal contractors who fail to disclose that they've been hacked or who fail to meet cybersecurity standards. "We have experienced where companies do not pay the attention they need to on this front," Monaco said. Ransomware attacks have flourished even as the federal government grapples with more old-fashioned, albeit sophisticated, cyber espionage. The Justice Department was among the agencies hit hard by the SolarWinds breach, in which Russian government hackers exploited a supply chain vulnerability to gain access to the networks of federal departments and private companies. The Justice Department has said more than two dozen U.S. attorneys' offices had at least one employee whose email account was compromised. It was a reminder, she said, that no one is immune from a sophisticated breach. "We need to practice what we preach and be doing the same type of vigilance on our cybersecurity that we are asking companies to do," she said.
Return to Top	

HEADLINE	**11/03 US hijacks ransom site; group shuts down**
SOURCE	**https://www.washingtonpost.com/national-security/cyber-command-revil-ransomware/2021/11/03/528e03e6-3517-11ec-9bc4-86107e7b0ab1_story.html**
GIST	A major overseas ransomware group shut down last month after a pair of operations by U.S. Cyber Command and a foreign government targeting the criminals' servers left its leaders too frightened of identification and arrest to stay in business, according to several U.S. officials familiar with the matter. The foreign government hacked the servers of REvil this summer, but the Russian-speaking criminal group did not discover it was compromised until Cybercom last month blocked its website by hijacking its traffic, said the officials who spoke on the condition of anonymity because of the matter's sensitivity. Cybercom's action was not a hack or takedown, but it deprived the criminals of the platform they used to extort their victims – businesses, schools and others whose computers they'd locked up with data-encrypting malware and from whom they demanded expensive ransoms to unlock the machines, the officials said.

In the hours after the Cybercom operation, which has not been previously reported, one of REvil's leaders saw the site's traffic had been redirected.

"Domains hijacked from REvil," wrote 0_neday, an REvil leader, on a Russian-language forum popular with cyber criminals, on Oct. 17.

A "third party," he wrote – without knowing Cybercom was responsible – had cloned the group's webpage having obtained the private keys to its server, which is reachable only through Tor, a special browser that routes Internet traffic through a worldwide network of servers to anonymize the user's identity.

A first inspection did not turn up signs of compromise, 0_neday said on the forum.

Then he checked again, and this time what he found spooked him.

"The server was compromised," he wrote hours later, "and they are looking for me." And then: "Good luck everyone, I'm taking off."

Soon after, REvil ceased operations, such as recruitment of affiliates, ransom negotiations and distribution of malware.

The Washington Post previously reported that REvil's servers had been hacked in the summer, permitting the FBI to have access. The compromise allowed the FBI, working with the foreign partner, to gain access to the servers and private keys, officials said. The bureau was then able to share that information last month with Cybercom, enabling the hijacking, they said.

Cyber Command spokeswoman, Col. Sunset Belinsky, said: "As a matter of operational security, we wouldn't provide comment on cyber intelligence, planning, or operations."

Cybercom's leader, Gen. Paul Nakasone, said at the Aspen Security Forum Wednesday that while he wouldn't comment on specific operations, "we bring our best people together . . . the really good thinkers" to brainstorm ways to "get after folks" conducting ransomware attacks and other malign activities. "I'm pleased with the progress we've made," he said, "and we've got a lot more to do."

The group's departure may be temporary. Ransomware gangs have been known to go underground, regroup and reappear, sometimes under a new name. But the recent development suggests that ransomware crews can be influenced – even temporarily – to cease operations if they fear they will be outed and arrested, analysts say.

"The latest voluntary disappearance of REvil highlights the powerful psychological impact of having these villains believe that they are being hunted and that their identities will be revealed," said Dmitri Alperovitch, executive chairman of the think tank Silverado Policy Accelerator, and a cyber expert. "U.S. and allied governments should proudly acknowledge these cyber operations and make it clear that no ransomware criminal will be safe from the long reach of their militaries and law enforcement agencies."

Cybercom's operation came in the wake of high-profile REvil attacks. In June, REvil ransomed the world's largest meat processor, Brazilian company JBS, in an action that temporarily halted operations at its nine beef processing plants in the United States and caused disruptions at other facilities in Canada and Australia.

In July the group struck again, this time targeting Kaseya, a Miami-based IT firm, infecting its software updates with ransomware that spread to hundreds of businesses. In a post on REvil's "Happy Blog" site, the group initially demanded $70 million to provide a decryption key to unlock the files of businesses victimized by the attack.

REvil has disappeared before.

	In July, after the Kaseya hack, President Joe Biden warned Russian President Vladimir Putin that the United States would take "any necessary action" to defend critical infrastructure. Around the same time, another group member who went by the nickname "unknown"disappeared. Unknown's vanishing unnerved the group, and without warning, it went offline. It is unclear whether Biden's warning played any role in either. In any case, 0_neday explained in a post last month, "since there was no confirmation of the reason for his disappearance, we resumed our work, thinking he was dead." Privately REvil members were telling affiliates the group would return, according to Recorded Future threat intelligence analyst Dmitry Smilyanets, who closely tracks the group's activities. "They were telling people, 'Don't worry, everything's okay – we will be back,'" Smilyanets said. "It wasn't a secret in the community that the REvil brand would reemerge." REvil returned in September, picking up where it left off, recruiting new "affiliate" hackers to help it conduct attacks. Its victims included a plastics manufacturer and a legal aid service for the poor. Then Cybercom struck. Smilyanets said he believes "REvil as a brand is done." The malware developers and the hackers will keep doing what they have been doing, he predicted, but probably under a different name or for another group. As for 0_neday, Smilyanets predicts: "The guy will be back." Said Smilyanets: "He's so adept at cybercrime. He will not quit. He wants his millions of dollars."
Return to Top	

HEADLINE	**11/03 Official: unknown if Russia cracking down**
SOURCE	**https://therecord.media/too-early-to-tell-if-russia-has-cracked-down-on-ransomware-gangs-nakasone-says/**
GIST	The country's top military cyber official on Wednesday said that is too soon to know if the Kremlin has taken action against ransomware gangs operating on Russian soil. "I think it's too early to tell," Army Gen. Paul Nakasone, who leads U.S. Cyber Command and the National Security Agency, said at the Aspen Security Forum. It's been nearly five months since President Joe Biden demanded Russian leader Vladimir Putin crack down on ransomware operating with Russian territory. Following the meeting, the two created an experts group on cybersecurity where administration officials have provided the Kremlin with information about certain cyber criminals and conveyed what actions Washington expects the government to take against them. "We've seen some steps by the Russian government and are looking to see follow-up actions," a senior administration official told reporters last month before the White House held a two-day virtual ransomware summit. The official declined to elaborate. However, several senior officials across the government have publicly said they see no evidence of any change in Russian behavior and raised doubts that the Kremlin could, or would, act. Nakasone said more time was needed before rendering a verdict. "Let's let this play out," he said. "There's engagement going on." His remarks came the same day The Washington Post reported that Cyber Command and a foreign government launched operations that shut down the notorious digital group known as "REvil." The

	organizations is widely believed to operate out of Russia and was responsible for the ransomware attacks on meat processor JBS and software company Kaseya earlier this year. Naksone declined to comment on the article. He stressed that both of the agencies he leads have launched a "surge" to combat the proliferation of ransomware — which he has predicted would remain a top threat to the country's economic and national security for the next several years. "We bring our best people together" to figure out how to go after criminal operations, learn about their capabilities and go after their flow of illicit money, he said. "I would say we've made a lot of progress and I'm pleased with the progress that we've made and we've got a lot more to do," according to Nakasone.
Return to Top	

HEADLINE	**11/03 France: Lockean in attacks on companies**
SOURCE	**https://therecord.media/cert-france-lockean-ransomware-group-behind-attacks-on-french-companies/**
GIST	French cybersecurity officials have identified today for the first time a ransomware "affiliate group" that is responsible for a long list of attacks against French companies over the past two years. Identified as **Lockean**, the group's activities and modus operandi were detailed today in a comprehensive report published by France's Computer Emergency Response Team (CERT-FR), a division of ANSSI, the country's national cybersecurity agency. According to French officials, the group has been active since June 2020 and "has a propensity to target French entities," having been linked to attacks on at least seven French companies, such as transportation logistics firm **Gefco**, pharmaceutical groups **Fareva** and **Pierre Fabre**, and local newspaper **Ouest-France**. **Lockean operators used different ransomware strains** CERT-FR officials said the group would typically rent access to corporate networks that had been previously infected via Emotet phishing emails, where they would deploy the QakBot malware and later the CobaltStrike post-exploitation framework. Lockean operators would then use tools like AdFind, BITSAdmin, and BloodHound to move laterally inside a network in order to expand their access and control over a company's systems. The group would then use the RClone utility to copy sensitive files from the victim network and then deploy a file-encrypting ransomware strain. According to CERT-FR officials, who investigated several of these intrusions, the Lockean group used different ransomware strains across the years, such as DoppelPaymer, Maze, Egregor, REvil (Sodinokibi), and ProLock. **Second ransomware affiliate group identified** Because Lockean used different ransomware strains, officials believe the group is what security researchers call a "**ransomware affiliate**," a term that refers to criminal groups who sign up on Ransomware-as-a-Service (RaaS) platforms. Through these platforms, affiliates gain access to ready-to-deploy ransomware strains, which they deploy on hacked networks, splitting successful ransom payments with the ransomware's creators. If victims refused to pay, data from these companies would be published on so-called "leak sites" operated by the RaaS platforms, where victims would often be listed in order to ramp up public pressure on the hacked companies.

	Lockean is now the second ransomware affiliate group that has been publicly identified by law enforcement agencies after the FBI exposed the OnePercent group in August.
Return to Top	

HEADLINE	**11/04 GitLab servers exploited in DDoS attacks**
SOURCE	**https://therecord.media/gitlab-servers-are-being-exploited-in-ddos-attacks-in-excess-of-1-tbps/**
GIST	Threat actors are exploiting a security flaw in GitLab self-hosted servers to assemble botnets and launch gigantic distributed denial of service (DDoS) attacks, with some in excess of 1 terabit per second (Tbps). The DDoS attacks, disclosed today by Damian Menscher, a Security Reliability Engineer at Google Cloud responsible for Google's DDoS defenses, are exploiting CVE-2021-22205, a vulnerability that GitLab patched back in April 2021. **Attacks target GitLab's metadata removal feature** Discovered by William Bowling and reported to GitLab via its bug bounty program, the vulnerability impacts ExifTool—a library used to remove metadata from images uploaded on web servers. Under the hood, GitLab uses ExifTool inside GitLab Community Edition (CE) and Enterprise Edition (EE), the open-source and commercial versions of its service that companies can install on their own servers—for scenarios where they want to handle proprietary code in secure environments and can't use GitLab's cloud-based service. In a report filed via HackerOne, Bowling said he discovered a way to abuse how ExifTool handles uploads for DjVu file format used for scanned documents to gain control over the entire underlying GitLab web server. Attacks exploiting this vulnerability began in June this year, according to Italian security firm HN Security, who first reported signs of exploitation last week. At the time, HN security researcher Piergiovanni Cipolloni said the company began an investigation after spotting randomly-named users being added to compromised GitLab servers, users that were most likely created by the attackers to allow remote control of the hacked systems. While the purpose of these attacks remained unclear for HN Security, yesterday, Google's Menscher said the hacked servers were part of a botnet comprising of "thousands of compromised GitLab instances" that was launching large-scale DDoS attacks. **Around 30,000 GitLab servers remain unpatched** Just as seen in many other previous cases, the botnet operators appear to be exploiting the tardiness of companies across the world when it comes to patching their software, in this case, in-house GitLab servers. According to a Rapid7 analysis published on Monday, there are more than 60,000 GitLab servers connected to the internet, of which around half still remain unpatched for the CVE-2021-22205 ExifTool exploit. Public proof-of-concept code for this vulnerability has been available since June, around the same time that HN spotted the first attacks. Of note is that the ExifTool vulnerability at the core of the GitLab issue, tracked independently as CVE-2021-22204, might also impact other types of web applications where the tool might have been deployed, so it may be that additional exploitation is also likely reported, and that other types of web apps might need patching as well.

	The simplest way to prevent attacks would be to block the upload of DjVu files at the server level, if companies don't need to handle this file type.
Return to Top	

HEADLINE	**11/03 Sinclair broadcasting ransomware attack**
SOURCE	**https://www.cyberscoop.com/sinclair-broadcast-group-ransomware-ongoing-disruption-macaw/**
GIST	The ransomware attack on conservative broadcasting giant Sinclair is still causing problems, the company reported in a U.S. Securities and Exchange Commission filing Wednesday. Noting that the investigation is ongoing, the notice reports that the Oct. 17 intrusion "has not yet been fully resolved, and certain disruptions to … business and operations remain." The full extent of the impact on Sinclair's "business, operations and financial results is not known at the present time." Employees of the Maryland-based company — which is the second-largest broadcast company in the U.S., owning or operating 185 television stations in 85 markets, multiple national networks, and 21 regional sports network brands — reported at the time that the attack had caused "major technical problems" and made it difficult for some stations to get on the air. The company also reported that hackers had taken data in the attack. "Our employees' quick response and creative workarounds have helped us restore a significant portion of our systems," Chris Ripley, the company's president and CEO, said in the filing. "As we work to complete our investigation, we will look for opportunities to enhance our existing security measures." A statement issued by the company initially reported that local advertisements had been impacted, but didn't offer any additional detail. The Wednesday filing notes that although the company has insurance to "cover losses related to cybersecurity risks and business interruption, such policies may not be sufficient to cover all losses." Evil Corp, a prolific Russian cybercrime group that has been sanctioned by the US government, is believed to be behind the breach. Researchers blamed the group, saying it had used a new strain of malware called Macaw to target Sinclair, perhaps as a means to facilitate payments from U.S. targets that would otherwise be barred from paying ransoms. Macaw, which had also been used to target Japanese technology manufacturer Olympus just days before Sinclair, was the latest iteration of Evil Corp-associated malware, building off previous strains such as WastedLocker and others, researchers told CyberScoop. A Sinclair spokesperson did not immediately respond to a request for comment Wednesday.
Return to Top	

HEADLINE	**11/03 'Tortilla' wraps Exchange servers in attacks**
SOURCE	**https://threatpost.com/tortilla-exchange-servers-proxyshell/175967/**
GIST	A new-ish threat actor sometimes known as "Tortilla" is launching a fresh round of ProxyShell attacks on Microsoft Exchange servers, this time with the aim of inflicting vulnerable servers with variants of the Babuk ransomware. Cisco Talos researchers said in a Wednesday report that they spotted the malicious campaign a few weeks ago, on Oct. 12. Tortilla, an actor that's been operating since July, is predominantly targeting U.S. victims. It's also hurling a smaller number of infections that have hit machines in the Brazil, Finland, Germany, Honduras, Thailand, Ukraine and the U.K.… Prior to this ransomware-inflicting campaign, Tortilla has been experimenting with other payloads, such as the PowerShell-based netcat clone PowerCat.

Netcat is a networking utility for reading from and writing to network connections using TCP or UDP, designed to be a dependable back-end that can be used directly or easily driven by other programs and scripts.

PowerCat has a penchant for Windows, the researchers explained, being "known to provide attackers with unauthorized access to Windows machines."

ProxyShell's New Attack Surface

ProxyShell is a name given to an attack that chains a trio of vulnerabilities together (CVE-2021-34473, CVE-2021-34523, CVE-2021-31207), to enable unauthenticated attackers to perform remote code execution (RCE) and to snag plaintext passwords.

The attack was outlined in a presentation (PDF) given by Devcore principal security researcher Orange Tsai at Black Hat in April. In it, Tsai disclosed an entirely new attack surface in Exchange, and a barrage of attacks soon followed. August was glutted with reports of threat actors exploiting ProxyShell to launch webshell attacks, as well as to deliver LockFile ransomware.

In this latest ProxyShell campaign, Cisco Talos researchers said that the threat actor is using "a somewhat unusual infection chain technique where an intermediate unpacking module is hosted on a pastebin.com clone pastebin.pl" to deliver Babuk.

They continued: "The intermediate unpacking stage is downloaded and decoded in memory before the final payload embedded within the original sample is decrypted and executed."

Who's Babuk?

Babuk is a ransomware that's probably best known for its starring role in a breach of the Washington D.C. police force in April. The gang behind the malware has a short history, having only been identified in 2021, but that history shows that it's a double-extortion player: one that threatens to post stolen data in addition to encrypting files, as a way of applying thumbscrews so victims will pay up.

That tactic has worked. As McAfee described in February, Babuk the ransomware had already been lobbed at a batch of at least five big enterprises, with one score: The gang walked away with $85,000 after one of those targets ponied up the money, McAfee researchers said.

Its victims have included Serco, an outsourcing firm that confirmed that it had been slammed with a double-extortion ransomware attack in late January.

Like many ransomware strains, Babuk is ruthless: It not only encrypts a victim's machine, it also blows up backups and deletes the volume shadow copies, Cisco Talos said.

What's Under Babuk's Hood

On the technical side, Cisco Talos described Babuk as a flexible ransomware that can be compiled, through a ransomware builder, for several hardware and software platforms.

It's mostly compiled for Windows and ARM for Linux, but researchers said that, over time, they've also seen versions for ESX and a 32-bit, old PE executable.

In this recent October campaign though, the threat actors are specifically targeting Windows.

China Chopper Chops Again

Part of the infection chain involves China Chopper: A webshell that dates back to 2010 but which has clung to relevancy since, including reportedly being used in a massive 2019 attack against telecommunications providers called Operation Soft Cell. The webshell enables attackers to "retain access to an infected system using a client-side application which contains all the logic required to control the target," as Cisco Talos described the webshell in 2019.

This time around, it's being used to get to Exchange Server systems. "We assess with moderate confidence that the initial infection vector is exploitation of ProxyShell vulnerabilities in Microsoft Exchange Server through the deployment of China Chopper web shell," according to the Cisco Talos writeup.

The Infection Chain
As shown in the infection flow chart below, the actors are using either a DLL or .NET executable to kick things off on the targeted system. "The initial .NET executable module runs as a child process of w3wp.exe and invokes the command shell to run an obfuscated PowerShell command," according to Cisco Talos' report.

"The PowerShell command invokes a web request and downloads the payload loader module using certutil.exe from a URL hosted on the domains fbi[.]fund and xxxs[.]info, or the IP address 185[.]219[.]52[.]229," researchers said.

"The payload loader downloads an intermediate unpacking stage from the PasteBin clone site pastebin.pl," they continued – a site that "seems to be unrelated to the popular pastebin.com."

They continued: "The unpacker concatenates the bitmap images embedded in the resource section of the trojan and decrypts the payload into the memory. The payload is injected into the process AddInProcess32 and is used to encrypt files on the victim's server and all mounted drives."

More Ingredients in Tortilla's Infrastructure
Besides the pastebin.pl site that hosts Tortilla's intermediate unpacker code, Tortilla's infrastructure also includes a Unix-based download server.

The site is legitimate, but Cisco Talos has seen multiple malicious campaigns running on it, including hosting variants of the AgentTesla trojan and the FormBook malware dropper.

Babuk's Code Spill Helps Newbies
In July, Babuk gang's source code and builder were spilled: They were uploaded to VirusTotal, making it available to all security vendors and competitors. That leak has helped the ransomware spread to even an inexperienced, green group like Tortilla, Cisco Talos said.

The leak "may have encouraged new malicious actors to manipulate and deploy the malware," researchers noted.

"This actor has only been operating since early July this year and has been experimenting with different payloads, apparently in order to obtain and maintain remote access to the infected systems," according to its writeup.

With Babuk source code readily available, all the Tortilla actors have to know is how to tweak it a tad, researchers said: A scenario that observers predicted back when the code appeared.

"The actor displays low to medium skills with a decent understanding of the security concepts and the ability to create minor modifications to existing malware and offensive security tools," Cisco Talos researchers said in assessing the Tortilla gang.

Decryptor Won't Work on Variant
While a free Babuk decryptor was released last week, it won't work on the Babuk variant seen in this campaign, according to the writeup: "Unfortunately, it is only effective on files encrypted with a number of leaked keys and cannot be used to decrypt files encrypted by the variant described in this blog post."

Return to Top

HEADLINE	**11/03 QR codes offer scammers another avenue**

SOURCE	**https://www.scmagazine.com/analysis/cybercrime/qr-codes-offer-scammers-another-avenue-to-circumvent-traditional-email-security**
GIST	A recently discovered phishing campaign leveraged QR codes as a means to bypass malicious link detection mechanisms — and while this particular scam featured some fundamental flaws, the public's increased use of "quick response" barcodes since the start of the pandemic may be behind their recent abuse in scams. This use of QR codes in phishing activity is not an entirely novel concept, although Abnormal Security, whose researcher uncovered the campaign, did say that this campaign represented a bit of an evolution of the technique. "We've seen actors use fake QR codes in the past — QR code images that are actual hyperlinks to a phishing site — and we've seen actors use QR codes out in the real world to try and get people to go to a malicious website, but this is the first time we've seen an actor embed a functional QR code into an email," said Crane Hassold, director of threat intelligence at Abnormal Security. The malicious phishing operation, which ran from Sept. 15 through Oct. 13, was disclosed not long after the Better Business Bureau posted its own QR scam alert last July. According to the organization's warning, some weaponized QR codes are designed to redirect victims to an information or credentials phishing website, while others may trick users into launching a payment app or follow a malicious social media account. "These scams differ greatly, but they all have one thing in common. Scammers hope you will scan the code right away, without taking a closer look," the alert stated. Phishing scammers are constantly looking for avenues to elude solutions that scan for malicious URLs and attachments, including those employed by secure email gateways and other traditional email security solutions. QR codes are one such option — one that the BBB said it's been encountering more of lately. And there are two reasons for that. "First of all, they [QR codes] came back into widespread use due to the pandemic; having touchless options for menus, coupons, and other information helped reduce physical contact and the spread of the virus," said Katherine Hutt, chief communications officer with the International Association of Better Business Bureaus, Inc. "In addition, virtually all cellphone cameras can now read QR codes without downloading a separate app. Scammers are opportunists; if we're using QR codes, then of course they are using QR codes." And there's a psychological component to this attack strategy, as well: "We just aren't as careful about reviewing URLs on our phones as we are on our computers," Hutt continued. The QR-based phishing — or "quishing" — scheme detected by Abnormal Security attempted to collect Microsoft credentials, according to a company blog post written by threat intelligence analyst Rachelle Chouinard. The QR codes, in this case, purportedly gave the email recipient access to a missed voicemail. "All the QR code images were created the same day they were sent, making it unlikely that they have been previously reported and would be recognized by a security blocklist," stated the report. "In total, six unique profiles were used to send messages for the campaign, with most designed to appear related to the same industry as the target." The attackers send the emails from compromised Outlook accounts, and hosted the phishing pages by leveraging an enterprise survey service, plus Amazon and Google services. "The use of the QR code presents a unique challenge to those security platforms that look for known bad, as these emails come from legitimate accounts and contain no links, only seemingly benign images appearing to contain no malicious URLs," Chouinard writes in the blog post. "It's only by understanding that the account is compromised — combined with an understanding of the intent of the email — that this new and fairly innovative attack type can be detected."

	Fortunately, the campaign had a significant logic defect that likely reduced its efficacy: If you open up an email with your phone, what are you using to scan the imagine? "The practical aspects of getting a target to scan a QR code with a separate device seem to create a barrier that would result in a relatively low success rate," said Hassold. There are also tactics and technologies companies can employ to identify such scams when they surface. "By looking at the emails in a more holistic and behavioral manner, these malicious messages can be identified, which is how Abnormal was able to detect them before they reached our customers' inboxes," said Hassold. Indeed, Abnormal reported blocking nearly 200 emails featuring the malicious QR codes by sniffing out the use of compromised accounts and detecting potentially suspicious activity through the analysis of unique sender data and email content. "We believe that because phishing is a human and machine problem, the only way to solve it is with a human and machine solution that leverages the power of AI on the machine side, combined with the power of highly targeted training for employees on the human side, added Eyal Benishti, CEO at Ironscales. Benishti believes "computer vision" technology in particular would be useful for stopping these attacks. "QRs can be easily translated into a link and scanned by email security solutions with computer vision capabilities," he explained, "so we feel it's likely a seasonal attack that will diminish as solutions with computer vision are able to detect and thwart the potential attacks." "Education is the best preventative measure," added Hutt, noting that the BBB recently launched a website to help people recognize common scams that they might encounter. "Remember, the topics change with whatever is current or in the news, but the tactics themselves are remarkably similar year after year," Hutt continued. "Generally, scammers are pretending to be someone they are not in order to get money or personally identifiable information from you. If they steal your PII, they can sell it many times over, or they can pretend to be you in order to scam someone else."
Return to Top	

HEADLINE	**11/03 Holiday shopping: retail bot attacks surge**
SOURCE	**https://www.infosecurity-magazine.com/news/holiday-disruption-retail-bot/**
GIST	Security experts have warned of potential disruption to the upcoming holiday shopping season after recording a double-digit year-on-year increase in bot-driven cyber-attacks so far in 2021. Imperva's *State of Security Within eCommerce* report revealed that over half (57%) of attacks targeting retail websites this year were carried out by bots, versus just 33% across other industries. Account takeover attempts, looking to hijack customers' accounts to steal personal and financial info, reached 33% so far in 2021, versus 26% across other verticals. These attacks are often carried out by what Imperva describes as "sophisticated" bots, capable of mimicking human mouse movements and clicks to defeat retailers' cyber-defenses. They're responsible for account takeover and denial of inventory, where items are added to account baskets to take them out of circulation, making them unavailable for legitimate customers. This could exacerbate existing supply chain issues that threaten stock availability this holiday season, warned Imperva director of technology, Peter Klimek. "With the global supply chain conditions worsening, retailers will not only struggle to get products to sell in Q4 but will face increased attacks from motivated cyber-criminals who want to benefit from the chaos," he argued.

	"Imperva Research Labs' data underscores the need for retailers to invest in security that spans from edge to applications and APIs all the way to the data. Only by protecting all paths to data can retailers truly defend their critical systems and the consumers who rely on them." To that end, Imperva also recorded a surge in DDoS attacks, including a 200% month-on-month increase in September 2021. The vendor warned that as retailers build out their website functionality with chatbots and web analytics and connect customers via API to features such as product search and order fulfillment tracking, their cyber-attack surface will continue to expand.
Return to Top	

HEADLINE	**11/03 Mobile phishing attacks energy sector rise**
SOURCE	**https://www.bleepingcomputer.com/news/security/mobile-phishing-attacks-targeting-energy-sector-surge-by-161-percent/**
GIST	Mobile phishing attacks targeting employees in the energy industry have risen by 161% compared to last year's (H2 2020) data, and the trend is showing no signs of slowing down. Although the perils of outdated and vulnerable devices plague all sectors, a new report by cybersecurity firm Lookout indicates that energy is the most targeted, followed by finance, pharma, government, and manufacturing. In terms of geographic targeting, Asia-Pacific tops the list, followed by Europe and then North America. However, there is a rising trend in phishing attacks targeting the global energy industry across the world. Mobile phishing also surged in the first half of 2021, with nearly 20% of all employees in the energy sector being targeted in mobile phishing attacks, leading to an increase of 161% over the previous six months. VPN credentials harvesting With so many people working from home due to the COVID-19 pandemic, many employees use VPNs to access corporate networks. Unfortunately, this remote access to a corporate network makes for an attractive target for threat actors, who use phishing to steal VPN credentials or domain credentials. In 67% of all analyzed phishing cases by Lookout researchers, threat actors are performing credential theft. To conduct these campaigns, the attackers employ email, SMS, phishing apps, and login pages at fake corporate sites. These credentials enable them to gain access to internal networks, which can then be used for further lateral movement and finding additional pivoting points. From there, they can locate vulnerable systems and launch attacks against industrial control systems which typically carry unidentified flaws for years. The Android problem According to the report from Lookout, the most significant attack surface stems from 56% of Android users running out-of-date and vulnerable versions of the OS. "Outdated versions of Google and Apple operating systems are still in use across the energy industry. Old versions expose organizations to hundreds of vulnerabilities that can be exploited by bad actors seeking access to an organization's environment," explains the report from Lookout. A full year after Android 11 was released, Lookout's telemetry showed that only 44.1% of active Android devices were using it.

	In contrast, iPhones are far less vulnerable to exploitation, as most iOS users are running the latest version. Some of the flaws in older Android versions are easily exploitable and pretty across the entire user base. For example, CVE-2020-16010 in Chrome can be trivially exploited through a specially crafted HTML page, and considering the browser's popularity, would be exposed on all outdated Android phones. Riskware is a bigger problem than malware Apps that request risky permissions and access sensitive data on the device are now a bigger problem than "pure" malware, as they are far easier to pass through app store vetting. Many of these apps connect to obscure servers and send various types of data that are irrelevant to their core functionality but which still constitute a great risk to the user and their employing organization. Spyware, keyloggers, trojans, and even ransomware droppers remain a problem, but it's more likely to see these deployed in highly targeted attacks, so their distribution volumes are significantly smaller. As such, employee training is critical in minimizing security lapses, as the human factor remains the greatest risk for installing riskware and the clicking/tapping of suspicious links. Lookout reports that a single session of anti-phishing training results in 50% fewer clicks onto phishing links for the next 12 months.
Return to Top	

HEADLINE	**11/03 Stealthier version Mekotio banking trojan**
SOURCE	**https://www.bleepingcomputer.com/news/security/stealthier-version-of-mekotio-banking-trojan-spotted-in-the-wild/**
GIST	A new version of a banking trojan known as Mekotio is being deployed in the wild, with malware analysts reporting that it's using a new, stealthier infection flow. The last notable activity of Mekotio dates back to the summer of 2020 when the trojan's operators deployed it in a campaign targeting Latin American countries. The targeting scope appears to be the same in recent attacks, with Spanish being the language of choice for the phishing emails that start the infection chain. **A new attack flow** The infection begins with a phishing email bundling a ZIP attachment containing an obfuscated batch script that fetches and executes a PowerShell script. Once the PowerShell script gets launched, it will download a second ZIP archive after some basic location and anti-analysis checks. If the checks confirm the victim is in Latin America and the malware isn't running on a virtual machine, the second ZIP, which contains the Mekotio payload in DLL form, is extracted. Multi-step attack flows like the one above may appear unnecessarily complicated, but they're needed to evade detection and successfully deploy the final payload. One of the advantages of modular attacks is the added ability to make subtle changes that render previous detection methods useless. This is precisely the case in Mekotio's development, as the trojan's code has largely remained unchanged, with its authors mostly tweaking things instead of adding new capabilities.

Same old code in new wrapping

The three novel elements that make the latest Mekotio version harder to detect are the following:

- A stealthier batch file with at least two layers of obfuscation
- New file-less PowerShell script that runs directly in memory
- Use of Themida v3 for packing the final DLL payload

CheckPoint reports seeing approximately 100 attacks in the past three months deploying cipher substitution techniques, which albeit simple, help Mekotio go undetected by most AV products.

The second layer of obfuscation is slicing the PowerShell commands into parts saved in different environment variables and then concatenating the values during execution.

The trojan's primary goal remains to steal people's e-banking credentials and online account passwords. Some past Mekotio variants could also hijack cryptocurrency payments and direct them to actor-controlled wallets, but recent versions have removed this functionality.

CheckPoint says the new campaign was launched right after the Spanish Civil Guard arrested 16 people in Mexico, linked with local Mekotio distribution.

However, the core Mekotio crew appears to be based in Brazil, and it's assumed that they are Mekotio's creators who are now selling it to other cybercriminals.

ESET characterized this particular trojan as "chaotic" last year due to the concurrent development that resulted in the simultaneous circulation of different variants.

That activity has now waned, and the most recent campaign uses the variant analyzed by CheckPoint.

Return to Top

HEADLINE	11/03 BlackMatter moves victims to LockBit
SOURCE	https://www.bleepingcomputer.com/news/security/blackmatter-ransomware-moves-victims-to-lockbit-after-shutdown/
GIST	With the BlackMatter ransomware operation shutting down, existing affiliates are moving their victims to the competing LockBit ransomware site for continued extortion. This morning, news broke that the BlackMatter ransomware gang is shutting down after members have gone missing and increased pressure by law enforcement. As part of this shutdown, the ransomware operators are allowing affiliates to receive decryptors for existing negotiations so that they can continue extorting victims. While BlackMatter's infrastructure is still live, BleepingCompuer has learned that affiliates are moving existing victims to the LockBit ransomware negotiation site. In existing BlackMatter negotiation chats, affiliates are providing victims links to LockBit's Tor sites where new negotiation pages have been setup for them. At these LockBit negotiation pages, the BlackMatter affiliates continue to negotiate with victims to receive a ransom payment. As for BlackMatter, they are continuing their shut down, with today's activities being to delete their presence from Russian-speaking hacking forums. Security researcher pancak3lullz has been following BlackMatter's cleanup activities, showing that the gang withdrew 4 Bitcoins (~$250,000) today from the Exploit hacking forum and deactivated their account.

	The gang has also been editing their existing posts on forums and asking moderators to delete them. With REvil and BlackMatter now shut down, LockBit has become one of the largest and most successful ransomware operations running today. The LockBit representative known as 'LockbitSupp' has shown to be a savvy threat actor who constantly adjusts tactics to recruit new affiliates, especially as established operations shut down. While BlackMatter will likely rebrand and return as a new ransomware operation, their partnership with LockBit may hurt them in the long run as they lose experienced affiliates.
Return to Top	

HEADLINE	**11/03 CISA new directive for patching**
SOURCE	**https://www.darkreading.com/vulnerabilities-threats/cisa-issues-new-directive-for-patching-known-exploited-vulnerabilities**
GIST	The US Cybersecurity and Infrastructure Security Agency (CISA) has issued a new directive that will now require federal agencies to patch known exploited vulnerabilities within specific time frames. CISA has published a catalog listing approximately 290 vulnerabilities going back to 2017 that threat actors are currently actively exploiting in attacks against federal entities and other organizations. The catalog sets hard deadlines — some as soon as Nov. 17 — within which federal agencies are required to patch them. CISA will update the catalog on a continuing basis with information on new vulnerabilities that attackers might be exploiting and that also present certain specified minimum levels of risk to federal agencies. The agency — which is part of the US Department of Homeland Security — described its Binding Operational Directive (BOD) 22-01 as designed to get federal agencies to address more quickly those vulnerabilities that are known to pose significant risk. "It is essential to aggressively remediate known exploited vulnerabilities to protect federal information systems and reduce cyber incidents," the DHS said in an advisory on Wednesday. CISA's directive applies only to vulnerabilities on information systems belonging to civilian federal agencies that are hosted on agency premises or by third parties on the agency's behalf. But private sector organizations can use the catalog and patching deadlines to improve their vulnerability management practices and reduce exposure to cyberattacks. The new directive reflects the high level of concern within government and the private sector over attacks like the supply chain assaults involving SolarWinds and Kaseya and campaigns that exploited vulnerabilities in Microsoft Exchange, Pulse VPN, and other VPN products over the past year. The attacks affected a wide number of organizations and often involved vulnerabilities that organizations should have known about and patched against long ago. Jamil Jaffer, former associate White House Counsel to President George W. Bush and current senior vice president at IronNet, says CISA's directive is not entirely a surprise given the current threat environment. "We have seen a number of large-scale incidents take place, including the Solar Winds hack and increased Nobelium activity noted recently by Microsoft," he says. "We've known for a long time that our private and public sectors are targeted by sophisticated nation-state attackers.' and it's no surprise that the federal government is trying to get their own house in order." Building on Previous Directives

CISA's latest directive builds on two earlier directives that it issued around vulnerability patching. The first in May 2015 required federal agencies to mitigate known "critical risk" vulnerabilities within 30 days of the flaws being publicly disclosed. At the time, the agency described the move as being fueled by concern over the length of time it took agencies — sometimes even 300 days — to fix critical security issues.

CISA issued a second BOD in April 2019, which reduced the time frame for fixing critical issues to 15 days. The directive also put a deadline for less severe but still "high risk" vulnerabilities to be patched in 30 days. CISA's 2019 directive was spurred by concerns over the growing speed at which attackers were exploiting freshly disclosed flaws and by a massive increase in the number of critical and high-risk vulnerabilities being disclosed.

The latest directive takes CISA's vulnerability management strategy in a new direction: Instead of focusing just on vulnerabilities with high severity scores on the CVSS scale, the new directive sets specific patching deadlines for any vulnerability — critical, high, medium, or low severity — that is being actively exploited in attacks.

CISA said its decision is based on the fact that Common Vulnerability Scoring System (CVSS) scores alone are not an indication of the threat a specific flaw might present to organizations. Increasingly, attackers have begun chaining together flaws of varying severity in their attacks, CISA said.

For example, the agency pointed to the so-called ProxyLogon set of four flaws in Microsoft Exchange Server that Russia's Nobelium group and others have exploited in a wave of attacks earlier this year. In these attacks, threat actors used relatively low-severity flaws to gain an initial foothold on a target network and then incrementally elevated privileges by abusing additional vulnerabilities.

"I anticipate this is one of many actions we will see in the coming months to improve the security posture of federal civilian agencies," says Allie Mellen, an analyst at Forrester Research.

Earlier this year, President Biden issued an executive order that, among other things, imposed new threat monitoring requirements for federal agencies. CISA's directive focuses on improved cyber hygiene another essential component of threat defense. "[The directive] speaks to the importance of getting the basics right first and on an ongoing basis. We talk about the importance of patching a lot — and now we have the directive to start enforcing it," Mellen notes.

Challenging Task

Many of the known exploited vulnerabilities in the new CISA catalog have patching deadlines of May 3, 2022. But numerous others have a Nov, 17 deadline meaning federal agencies have just 14 days to address the flaws. That deadline could be challenging for agencies to meet considering the amount of work that is likely required, security experts said.

"The CISA deadlines are somewhat arbitrary but are a good example of what every cybersecurity team should be doing on their own," says Yaniv Bar-Dayan, CEO and co-founder of Vulcan Cyber.

The effort should be to identify and prioritize cyber-risk, then implement an achievable plan to mitigate the vulnerabilities that pose the most risk to the business. "No doubt vulnerability remediation is a difficult, dirty job. If it wasn't, and our cyber hygiene was perfect, CISA wouldn't bother us with a list of known vulnerabilities like this, he says.

Bud Broomhead, CEO at Viakoo, says federal agencies are likely to face the biggest challenge in IoT and OT environments where remediation has been a larhely manual process till recently. "Agencies will have to bring in new technologies to deal with the scale and complexity," he predicts. "It will be virtually impossible to meet these deadlines using manual methods of patching systems."

	IronNet's Jaffer says CISA's directive makes clear that this is an initiative the government wants federal agencies to execute and complete on an urgent basis. But the short time frame for addressing some of the flaws will likely make compliance challenging for agencies — some more so than others. "For operational directives, CISA has a process whereby departments and agencies are required by law to develop a plan to comply — and ultimately comply — with binding operational directives," Jaffer says. An escalation process exists for prioritizing the issue in case an agency fails to comply by deadline. DHS/CISA will be responsible for using this process to put pressure on agency heads to ensure the directives are met. "In addition, Congress might raise pressure by requesting briefings and reports on how agencies are doing on meeting the directive requirements, including through the Government Accountability Office," he notes. Forrester's Mellen says that CISA will likely be reporting status of these requirements up to Secretary of Homeland Security, the Director of the Office of Management and Budget, and the National Cyber Director. "This is another step establishing CISA as the de facto leader on security in the federal government," Mellen adds, "especially with regards to civilian agencies."
Return to Top	

HEADLINE	**11/03 Scanning web to uncover malware infections**
SOURCE	**https://www.darkreading.com/security-monitoring/researchers-scan-the-web-to-uncover-malware-infections**
GIST	SECTOR CONFERENCE — Attackers scan the Internet for vulnerable servers and software. Security firms and universities often scan for open ports and misconfigurations. One security firm is now scanning to detect malware compromises. In a presentation today at the Toronto-based SecTor security conference, Marc-Etienne Léveillé, senior malware researcher for ESET, outlined how the company created its own scanning capability to aid in its research of infected systems. Through its analysis of the Kolabos malware late last year, ESET figured out a two-step scan that could detect an infected system and was able to notify affected companies, he said. While Internet scanning systems are common, Léveillé argued that being able to survey the entire Internet gives a company both context on current threats and the ability to dive into specific attacks. "We are frequently faced with a single malware sample that we don't have a lot of context around," he said. "We don't necessarily know who the actors have targeted or the industry — this is especially true on non-Windows platforms because of the lack of telemetry on those products." Dozens of companies and universities regularly scan the Internet to detect misconfigured devices, vulnerable systems, and exposed applications. Device search engine Shodan is perhaps the most well-known company to scan for open ports and vulnerabilities on the public Internet, but so do other organizations, such as Rapid7 through its Project Sonar and University of Michigan startup Censys, which aims to create a map of the evolving Internet of Things (IoT). The University of Michigan, which created the Zmap tool used by most Internet surveys, isn't alone. The University of Chicago and University of Pennsylvania are among the other academic institutions that regularly scan the Internet for research purposes. However, public services don't have the flexibility necessary for malware research, ESET's Léveillé said in an interview following the presentation. "We did work with Censys and Shodan before, and we are grateful they dedicated resources in running scans based on the indicators we gave them," he said. "However, we wanted to be independent and not

	have to bug them every time we wanted to perform a new scan or do a r-scan. Using our own system enables us to also perform scans using custom modules to fingerprint malware using nonstandard protocols." Léveillé and the ESET research team regularly take in-depth looks at malware, attempting to discover how far a particular malicious operation has spread. While the tools to stand up an Internet-wide survey are publicly available, creating a system from the ground up is not without its challenges. The first hurdle: finding an Internet service provider that would allow scanning from its network. "Internet service providers don't like scanning of their networks, but relying on third parties to run scans for us adds overhead and limits our capabilities," he says. Four ISPs rejected ESET's proposal before the company found a service provider willing to work with it. Since mid-2020, ESET has used the scanning system nearly 20 times to investigate specific malware families, including research published in January detailing the Kolabos malware that infected Linux servers and a project report published in August describing multiple backdoors in Microsoft's Internet Information Server (IIS). While other companies regularly use Internet scanning to enumerate specific devices, open ports, or misconfigurations, ESET's method is far more targeted, says Léveillé. "We do not, at this time, regularly scan and categorize IP addresses to be part of a threat group infrastructure," he says. "[However], fingerprinting and scanning for malware command-and-control servers is something we've successfully done, so it would be possible to automate the process and enrich our existing dataset in the future." In many ways, ESET and other organizations are in a race because they're not the only ones surveying the Internet landscape. In 2014, a group under the name Internet Scanning Project aggressively scanned Internet servers, and similar efforts have continued with the problem growing worse. Following a vulnerability disclosure, for example, scans that attempt to reveal the security issue will start within 15 minutes — and sometimes in as little as five minutes for a high-profile vulnerability, Palo Alto Networks stated in a 2021 analysis. "The ease of scanning [has given] rise to a cottage industry of analysts and criminals who scan for vulnerabilities and infrastructure — especially in the age of ransomware," the company stated in its report. "In the past five years, attackers have perfected techniques that scale at speed." Companies should focus on reducing their attack surface and recognizing that scans are usually the first step in attacking network devices, Palo Alto Networks advised.
Return to Top	

HEADLINE	**11/02 Ransomware operations continue to evolve**
SOURCE	**https://www.govinfosecurity.com/7-trends-how-ransomware-operations-continue-to-evolve-a-17841?&web_view=true**
GIST	Ransomware continues to be many criminals' weapon of choice for reliably shaking down victims small, medium and large, in pursuit of a safe, easy and reliable payday. But the ransomware landscape itself continues to evolve in numerous ways. For example, the arrival of new players remains constant, while big names occasionally bow out. Some gangs run complex ransomware-as-a-service operations, tapping specialists in network penetration, negotiations, malware development and more. Many others, however, lack the budget and staffing necessary to reliably take down big targets, so they operate on the periphery. And while many operations run their own data-leak sites, even these come with operational challenges.

As ransomware attacks continue, here are seven ways the ecosystem continues to evolve:

1. Groups Rise and Fall
Security firms continue to track a steady amount of churn in the ransomware-attacker space, including an influx of fresh faces or at least names.

Going dark in Q3 were Avaddon, Noname, relative newcomer Prometheus and REvil, aka Sodinokibi. But REvil returned in September, before disappearing again, last month, potentially due to being disrupted by law enforcement authorities.

Also in Q3, new players - or at least names - appeared, including
CryptBD, Grief, Hive, Karma, Thanos and Vice Society, Cisco Talos security researchers David Liebenberg and Caitlin Huey write in a blog post.

2. Rebranding Is Common
Some of those supposedly new operations, however, may simply be existing groups that rebranded. In Q3, for example, "the SynAck ransomware group, which hosted a data leak site called 'File Leaks,' rebranded itself as 'El_Cometa,'" Ivan Righi, a cyberthreat intelligence analyst with Digital Shadows, says in an analysis of Q3 trends.

"The DoppelPaymer ransomware was found to likely have rebranded as the 'Grief' ransomware group, and it is believed that the Karma ransomware group is a rebrand of the Nemty ransomware gang," he adds.

3. Attacks Spread Among Many Groups
Regardless of names, a greater number of players in Q3 appeared to be involved in a greater volume of the attacks being seen, the Cisco Talos researchers say. In particular, of the incident response engagements Cisco Talos worked, only Vice Society and REvil were seen across more than one engagement, they say, "highlighting greater democratization of emerging ransomware variants."

Not seen by Cisco Talos during any engagement, despite previously having been prolific: Ryuk. "Many security researchers believe the Conti ransomware family is a successor to Ryuk, potentially explaining the decline in observations of Ryuk activity," Liebenberg and Huey of Cisco Talos say.

Those findings largely square with what other firms have been recording. Ransomware incident response firm Coveware, for example, recorded a sharp rise in Conti attacks and a decrease in Ryuk attacks, based on thousands of cases with which it assisted during Q3. Because the firm helps victims with incidents that do not always become public, it's likely one of the more accurate assessments of what's actually happening in the wild.

Rank	Ransomware Type	Market Share %	Change in Ranking from Q2 2021
1	Conti V2	19.2%	+1
2	Mespinoza	11.3%	+2
3	Sodinokibi	8.9%	-2
4	Lockbit 2.0	8.4%	New in Top Variants
5	Hello Kitty	5.4%	-
6	Zeppelin	4.4%	+3
7	Ranzy Locker	3.0%	New in Top Variants
8	Suncrypt	2.5%	New in Top Variants
8	Hive	2.5%	New in Top Variants
9	Ryuk	2.0%	-3
9	BlackMatter	2.0%	New in Top Variants

Top 10 market share for ransomware strains seen in attacks in Q3 (Source: Coveware)

4. Ransomware Operators Are Not All Big Earners

A large number of ransomware groups appear to remain active. Just since Oct. 25, for example, Israeli threat intelligence firm Kela reports that 11 groups have listed victims on their data leak portals: Avos Locker, BlackByte, BlackMatter, Clop, Conti, Grief, LockBit, Marketo, Midas, Pysa and Xing.

Some are bagging big bucks. During Q3, when a business, government agency or any other organization opted to pay a ransom, on average it paid $140,000, according to Coveware, based on thousands of cases it helped investigate. While that average remained steady from Q2, it notes that in the same time frame, the median payment increased by more than 50%, suggesting that attackers have begun to focus more on smaller and midsize victims, after the Biden administration this past summer announced a crackdown on ransomware.

But McAfee researcher Thibault Seret, in a blog post, notes that not every ransomware-as-a-service operation is seeing six-figure ransom payoffs, or more.

"Going by recent headlines you could be forgiven for thinking all ransomware operators are raking in millions of ill-gotten dollars each year from their nefarious activities," he says. "Lurking in the shadows of every large-scale attack by organized gangs of cybercriminals, however, there can be found a multitude of smaller actors who do not have access to the latest ransomware samples, the ability to be affiliates in the post-DarkSide RaaS world or the financial clout to tool up at speed."

5. Malware Leaks Feed Smaller Players

But smaller operations can be innovative in other ways. For example, Seret details how the June leak of the builder for Babuk ransomware was seized on by some as a building block for rolling their own, more advanced crypto-locking malware.

But in another case, he says, attackers previously tied to .NET ransomware called Delta Plus simply tweaked the Babuk ransom note - inserting bitcoin wallet addresses that they, not Babuk, controlled, for victims to pay a ransom - and then used it to target victims. With this new, albeit only slightly tweaked

malware, he notes, the attack group began demanding ransoms not worth hundreds of dollars, but rather thousands.

6. Leaking Stolen Data Brings Challenges
While stealing data from a victim and threatening to leak it is a strategy widely practiced by ransomware gangs, it's not foolproof. Challenges are that a victim may of course still opt to not pay - and if an attacker didn't steal sensitive data, perhaps even more so. In addition, hosting the data also turns out to be fraught with challenges, Digital Shadows' Righi says in a blog post.

"Many ransomware groups have experienced difficulties managing data leak sites and hosting data on the dark web for download," he says. "This has resulted in some ransomware groups exposing data using public file-sharing websites, such as Mega[.]nz or PrivatLab[.]com. As these services are hosted on the clear web, they can often be taken down, and most download links are removed within a day or two."

Another challenge, he notes, is that dark web sites - meaning sites only reachable via the anonymizing Tor browser - are designed to prioritize privacy over performance. Therefore, navigating the dark web can be slow, and attempting to download leaked data can be an exercise in frustration.

Or at least that's what many users of the XSS Russian-language cybercrime forum reported, when they attempted to download data leaked in March by the Clop ransomware operation, which had stolen it from security firm Qualys.

"The download speeds were so slow that some users claimed it took them nearly one week to download the first dataset, while other users reportedly gave up," Righi says.

Hosting data leak sites and payment portals also makes them a target for law enforcement agencies. That's what appears to have happened to REvil, when an administrator rebooted the operation's Tor-based sites, only to find that someone else - perhaps a former administrator, perhaps a law enforcement official, perhaps both - also had a copy of the setup files, allowing them to hijack REvil's Tor sites (see: *Ransomware Soap Opera Continues With REvil's Latest Outage*).

7. Operators Risk Unmasking
Some ransomware operations appear to be especially big earners, thanks in part to some victims paying cryptocurrency ransoms worth millions of dollars.

Last week, weekly German newspaper Die Zeit reported that German police believe they've identified a suspected leader of REvil, a self-described bitcoin entrepreneur called "Nikolay K." - not his real name - thanks in part to tracing cryptocurrency tied to an attack by GandCrab, which was REvil's former incarnation. Police reportedly identified him after following $17,000 worth of cryptocurrency believed to have been paid to GandCrab in 2019 by one of its victims, the Staatstheater in Stuttgart, and finding it was tied to an email account used by Nikolay K.

If he is a REvil administrator, Die Zeit reports, that would help explain a lavish lifestyle, documented on social media by his wife, that includes yacht holidays, a luxury Vanguard Encrypto watch on his wrist and a high-end BMW in the driveway.

But a ransomware-driven lifestyle and attempts to remain anonymous might also take their toll on practitioners.

On Oct. 22, for example, the administrator of Groove ransomware, who goes by Orange - as well as TetyaSluha and boriselcin, for Russia's first elected president, Boris Yeltsin - posted a message on Groove's data leak site, claiming the whole effort had been an experiment designed to "troll" Western media. The message was cross-posted by boriselcin on the XSS cybercrime forum.

	His posts "claimed that there is no such thing as the Groove gang, and that behind the whole affair was one person, who has worked with many ransomware affiliate programs, including BlackMatter, LockBit and others," Victoria Kivilevich, director of threat research at Kela, tells Information Security Media Group. "The author claims that he was asked to write an article about mass media manipulation, and the Groove site was created just for that." John Fokker, the principal engineer and head of cyber investigations for Advanced Threat Research at McAfee Enterprise, recommends treating all criminal claims with a heavy dose of skepticism. "Regardless if Groove is a hoax or not, they or he - Orange - can be linked to multiple breaches. So it is definitely not a hoax for the victims," he says (see: *Ransomware Evolves: Affiliates Set to Wield Greater Power*). The propensity of some ransomware ringleaders to vent via posts to Russian-language cybercrime forums, rather than simply taking their earnings and quietly exiting, also suggests they're under increased stress to maintain the pace of operations, if not also their anonymity. "I think the emotions are indeed running high and if law enforcement starts cracking down, we can expect a lot more of these outbursts," Fokker says.
Return to Top	

HEADLINE	**11/03 UK Labour party hit by 'cyber incident'**
SOURCE	**https://www.theguardian.com/politics/2021/nov/03/labour-hit-by-cyber-incident-affecting-members-data?&web_view=true**
GIST	Labour has said it has been hit by a "cyber incident" that meant that a "significant quantity" of members' and supporters' data became inaccessible. The party said the impact of the incident, affecting an external supplier, was not yet clear and it was urgently investigating whether the data had been hacked. Police, cybersecurity specialists and regulators had been notified, it added. It is understood that it is unclear at this stage whether the party was specifically targeted, as opposed to merely being incidentally affected. Cybersecurity experts said it appeared to have the hallmarks of a ransomware attack, where hackers, often from Russia, demand money to restore access to data that has been seized and encrypted. "We are writing to you to let you know that a third party that handles data on our behalf has been subject to a cyber incident," Labour said in an email to supporters and members. "The third party told us that the incident had resulted in a significant quantity of party data being rendered inaccessible on their systems." Labour said the data affected "includes information provided to the party by its members, registered and affiliated supporters, and other individuals who have provided their information." The "full scope and impact" of the incident was being "urgently investigated". The party, which has about 430,000 members, routinely holds addresses, emails and other contact information for members, as well as some basic financial information such as direct debit details. Labour said it had already been in contact with the National Crime Agency, National Cyber Security Centre (NCSC), a division of GCHQ, and the Information Commissioner's Office, which regulates the handling of personal information. NCSC said it was aware of the issue and was assisting Labour. It said anybody "who thinks they may have been the victim of a data breach to be especially vigilant against suspicious emails, phone calls or text messages." The NCA confirmed it was leading the criminal investigation and said its inquiries were at an early stage. "We are working closely with partners to mitigate any potential risk and assess the nature of this incident," a spokesperson said.

	It is not the first time Labour has been affected by a cyber incident. Last year it said donor information had been stolen by a cybercriminal from a third-party provider called Blackbaud some time between February and May. Information stolen included names, email addresses, phone numbers and sums donated. Blackbaud, which provided a customer management system for the party, told Labour it had paid the ransom demanded by the cybercriminal and the company had received assurances that the data was destroyed as a result.
Return to Top	

HEADLINE	**11/03 Beware: Steam Discord free Nitro phishing**
SOURCE	**https://www.bleepingcomputer.com/news/security/beware-free-discord-nitro-phishing-targets-steam-gamers/?&web_view=true**
GIST	A new Steam phishing promoted via Discord messages promises a free Nitro subscription if a user links their Steam account, which the hackers then use to steal game items or promote other scams. The phishing scam is being conducted by many Discord accounts controlled by the threat actors or as automated bots that send other users links to what is supposedly a guide on how to receive Discord Nitro for free. "See, here free nitro 1 month, just link your Steam account and enjoy," reads the phishing messages… While this sounds like a promotional campaign (other than the grammar), the links take victims to a phishing site that the attackers made to look like a legitimate Discord page promoting the Nitro feature. After clicking on the "Get Nitro" button, a fake Steam login form is displayed, which looks almost identical to the legitimate form. In reality, the pop-up is a new window opened right on the phishing page, so whatever Steam credentials are entered are sent directly to the hacker's server. When attempting to login, victims are shown an error saying, "The account name or password that you have entered is incorrect," and prompts the user to log in again. This double-verification method ensures that no typing errors were made during the phishing process and that the stolen credentials are correct. **Nitro as bait** Discord Nitro is a paid membership plan on the popular VoIP and instant messaging platform, which comes with a set of highly sought-after account customization, content uploading, and server boost perks. Such is the popularity of Nitro that we've seen malware strains distributed using the same bait and even ransomware gangs asking for Nitro gift codes in return for a working decryptor. The latest scam analyzed by Malwarebytes is very similar to the one seen by BleepingComputer in the Summer of 2019. However, with that scam, threat actors used a "free game" as bait to serve victims with a fake Steam single sign-on page. As these landing URLs get reported and blacklisted, actors register new ones and move their malicious operations to new infrastructure, as shown by the list below shared by Malwarebytes.

	1nitro.club appnitro-discord.com asstralissteam.org.ru discord-steam-promo.com discordgifte.com dicsord-ticket.com discord-appnitro.com ds-nitro.com nitro-discordapp.com nitrodsgiveways.com steam-nitro.online **Domains used in the recent campaign.** *Source: Malwarebytes* Similarly, phishing lures are constantly changing with new lures to intrigue gamers with a promise for something free. With that said, when using Discord, users should be suspicious of any messages claiming to offer something for free if they click on an URL. There are no things offered for free outside the platforms themselves, so if Steam and Discord run a promotional campaign together, you would see it on either of the respective official apps/websites.
Return to Top	

HEADLINE	**11/03 US blacklists NSO Group over spyware**
SOURCE	**https://www.nytimes.com/2021/11/03/business/nso-group-spyware-blacklist.html**
GIST	In a remarkable breach with Israel over one of its most successful technology companies, the Biden administration on Wednesday blacklisted the NSO Group, saying the company knowingly supplied spyware that has been used by foreign governments to "maliciously target" the phones of dissidents, human rights activists, journalists and others. The firm, and another Israeli company, Candiru, acted "contrary to the national security or foreign policy interests of the United States," the Commerce Department said, a striking accusation against a business that operates under the direct supervision of the Israeli government. The ban is the strongest step an American president has taken to curb abuses in the global market for spyware, which has gone largely unregulated. The move by the Commerce Department was driven by NSO's export around the world of a sophisticated surveillance system known as Pegasus, which can be remotely implanted in smartphones. NSO's spyware has been under scrutiny for years for its ability to stealthily, and remotely, extract sound and video recordings, encrypted communications, photos, contacts, location data and text messages from a device — without so much as a single click. Among its targets were confidants of Jamal Khashoggi, the Washington Post columnist who was dismembered by Saudi operatives in Turkey; an array of human rights lawyers, dissidents and journalists in the Emirates and Mexico, and even their family members living in the United States. After a consortium of media outlets reported over the summer that NSO's spyware may have targeted smartphones belonging to journalists and world leaders from France, Morocco and elsewhere, a group of House Democrats called for NSO Group to be blacklisted and potentially sanctioned for human rights

violations. But it was never clear if those people were on a list of possible targets by NSO clients, or were actually hacked.

The announcement on Wednesday apparently came as a surprise to the Israeli defense ministry, which must approve licenses for the sale of Pegasus software to foreign governments, because it is categorized as a defense technology. While Israeli officials insisted they were unprepared for the move, which prohibits the firm from acquiring American technology, the Israeli government had received a string of official and private warnings from Washington.

The ministry of defense declined to comment on the record on the action. But there was no question that the Commerce Department, by placing the firm on the "Entity List" of blacklisted companies, was striking at the heart of the Israeli intelligence community. NSO's technology emerged from Unit 8200, Israel's highly secretive cyberunit, which has partnered with the United States around the globe, including in cyberoperations to disable Iran's nuclear facilities.

The ban would prohibit American firms from selling technology to NSO Group and its subsidiaries. Dell and Microsoft were alerted earlier that NSO Group would be added to the blacklist, according to two people briefed on the calls but unauthorized to speak publicly about them.

Cristin Goodwin, general manager of Microsoft's digital security unit, called the rule "a strong step toward addressing the danger these actors pose, and we encourage other countries to adopt similar policies."

After a series of revelations about NSO in The New York Times and other publications, the Biden administration warned that the surveillance software was being abused by authoritarian nations.

Two weeks ago, the Commerce Department added a new rule requiring U.S. companies to get a license to sell any intrusion software to foreign countries, an effort to curb the sale of surveillance tools to oppressive regimes like Saudi Arabia and the Emirates.

The announcement on Wednesday went one step further, taking direct aim at NSO Group, and signaling to its would-be investors, and acquirers, to stay away. The company had been mulling an initial public offering at a $2 billion valuation.

NSO said in a statement that it was "dismayed by the decision" and would ask for it to be reversed. The company has claimed — especially recently, as investigations proliferated — that it is pulling licenses for its software from governments that are using it to suppress dissent.

"Our technologies support U.S. national security interests and policies by preventing terrorism and crime," the company said.

The Biden administration concluded exactly the opposite.

Senator Ron Wyden, Democrat of Oregon, and one of the Senate's most outspoken voices on digital privacy, applauded the administration's move but argued it should go further.

"President Biden is sending a strong message that the U.S. won't stand for foreign hacking companies that violate human rights and threaten our national security," he said. He added that the administration should consider issuing sanctions under the Global Magnitsky Act.

Doing so would effectively freeze NSO's assets and force its largest investors, including Novalpina Capital, a British private equity firm — and its investors, which include Oregon's state pension fund — to divest. It could also thwart NSO Group's plans for a lucrative exit, such as an initial public offering or acquisition.

NSO was one of four companies that were blacklisted on Wednesday.

	Candiru, another Israeli firm, was sanctioned based on evidence that it supplied spyware to foreign governments. Positive Technologies of Russia, which was targeted with sanctions last April for its work with Russian intelligence, and Computer Security Initiative Consultancy of Singapore were added to the list for trafficking in hacking tools, according to the Commerce Department's announcement. "The United States is committed to aggressively using export controls to hold companies accountable that develop, traffic, or use technologies to conduct malicious activities that threaten the cybersecurity of members of civil society, dissidents, government officials and organizations here and abroad," Gina Raimondo, the commerce secretary, said in a statement. NSO has said it only sells its spyware to governments whose human rights records have been vetted, for the purpose of countering terrorism and crime. But its spyware continues to pop up on the phones of journalists, critics of autocratic regimes, even children. Some of NSO's targets — like Ahmed Mansoor, a critic of the United Arab Emirates — have been imprisoned and held in solitary confinement for years after NSO's spyware was found on their phones. Apple has patched its iOS software several times to mitigate vulnerabilities exploited by NSO's spyware. Candiru was founded by engineers who left NSO. Last July, Microsoft reported that Candiru's spyware exploited a pair of Windows vulnerabilities to target the phones, computers, and internet-connected devices of some hundred activists, journalists and dissidents across ten countries. Both NSO and Candiru were supposed to be under the strict control of Israel's Ministry of Defense. But the ministry authorized the companies to sell their products to a number of countries with a long history of severe human rights violations, like Saudi Arabia, and continued to approve their sale even after the murder of Mr. Khashoggi and the discovery of spyware on his associates' phones. In a brief response to the Times in September, the ministry said in a statement that it applied "even stricter" standards to exports than was required, and that "special emphasis" was placed on adhering to international agreements and protecting human rights. Whenever the ministry "discovers that the purchased item is being used in contravention of the terms of the license, especially after any violation of human rights, a procedure of cancellation of the defense export license or of enforcing its terms, is initiated," the ministry said. The Commerce Department clearly determined otherwise.
Return to Top	

HEADLINE	**11/03 Twitter misinformation backed Kenya leader**
SOURCE	**https://www.nytimes.com/live/2020/2020-election-misinformation-distortions?action=click&module=Well&pgtype=Homepage&section=Technology#researchers-say-a-coordinated-misinformation-campaign-on-twitter-backed-kenyas-president**
GIST	Last month, reporting on newly disclosed financial documents showed that Kenya's president, Uhuru Kenyatta, and members of his family were linked to 13 offshore companies with hidden assets of more than $30 million. The findings, part of the leaked documents known as the Pandora Papers, initially generated outrage online among Kenyans. But within days, that sentiment was hijacked on Twitter by a coordinated misinformation campaign, according to a new report published by the nonprofit Mozilla Foundation. The effort generated thousands of messages supporting the president, whose term is ending, and criticizing the release of the documents. "Like clockwork, an alternative sentiment quickly emerged, supporting the president and his offshore accounts," said Odanga Madung, a fellow at Mozilla and an author of the report. "Kenyan Twitter was awash in Pandora Paper astroturfing," he said.

	The research underscores how online platforms based in the United States still struggle to police inauthentic behavior abroad. Internal documents obtained by the former Facebook product manager turned whistle-blower, Frances Haugen, repeatedly showed how the social network failed to adequately police hate speech and misinformation in countries outside North America, where 90 percent of its users reside. Ann-Marie Lowry, a Twitter spokeswoman, said in a statement that the company's uniquely open nature empowered research such as Mozilla's. "Our top priority is keeping people safe, and we remain vigilant about coordinated activity on our service," Ms. Lowry said. "We are constantly improving Twitter's auto-detection technology to catch accounts engaging in rule-violating behavior as soon as they pop up on the service." Mr. Madung and another researcher, Brian Obilo, looked at over 10,000 tweets discussing mentions of Mr. Kenyatta in the Pandora Papers over a four-week period. They found a campaign of nearly 5,000 tweets with thousands of likes and shares that was "clearly inauthentic" and "coordinated to feign public support," according to the research. The 1,935 accounts that they found had participated in the campaign tweeted for days only about the Pandora Papers and Mr. Kenyatta, and got certain hashtags like #phonyleaks and #offshoreaccountfacts to appear on Twitter's dedicated sidebar for trending topics by posting the hashtag repeatedly. The researchers noted that many of the accounts they found had been part of a previous disinformation campaign tweeting pro-government propaganda from May that they had flagged to Twitter. The company took down some of the accounts but allowed others to remain up. "Before chest thumping and yawning mercilessly that H.E had stolen your money, know first when the offshore accounts were acquired #OffshoreAccountFacts," said one tweet that posted as part of the campaign, using a short hand for "His Excellency" to refer to Mr. Kenyatta. The post collected 341 likes and shares on Twitter before the account was suspended. A similar campaign was attempted on Facebook but the researchers found only 12 posts with under 100 interactions there, Mr. Madung said. After the researchers shared the report with Twitter's policy team, the company suspended more than 230 accounts for violating its platform manipulation and spam policies. It added that it would continue to work with third-party organizations that helped to identify tweets or accounts that violated the social network's policies.
Return to Top	

HEADLINE	**11/03 Report: cost of breach in energy, utilities**
SOURCE	**https://securityintelligence.com/articles/cost-data-breach-energy-utilities/**
GIST	On average, the cost of a data breach rose by 10% from 2020 to 2021. The energy industry ranked fifth in data breach costs, surpassed only by the health care, financial, pharmaceutical and technology verticals, according to the 17th annual Cost of a Data Breach Report. Some energy cybersecurity measures can help reduce the cost of a data breach in a big way. For example, take a look at zero trust deployments, artificial intelligence and automation. It's important to better understand data security in this growing and crucial field. Take a look at some recent data breaches that affected energy and utility providers. What data security risks and challenges are unique to these sectors? **What Is a Data Breach in the Energy and Utilities Industries?** The energy sector includes oil and gas companies, alternative energy producers and suppliers and utility providers such as electric companies. Energy cybersecurity breaches and failures can have tremendous impacts. They even go beyond the cost to the companies that mine for oil or gas or provide energy to customers. After all, people rely on these services for nearly every aspect of life.

Compromised Password Leads to Gas Shortages
This type of problem joined the United States' many other challenges in spring 2021. An attacker gained remote access to the network of a major U.S. pipeline company via an employee's virtual private network (VPN). The VPN was not even in use at the time. However, it remained open for threat actors to use it as a gateway to the company's main network. The attacker found the password used to access the account on a list of leaked passwords on the dark web. Experts suggest that the employee may have used the same password on another account. A threat actor then stole it from that account and shared it online.

One week after the data breach, the threat actor sent a ransom note. In response, the company shut the pipeline down. They did so on purpose because they wanted to avoid an attack on their operational technology network. After all, these are the systems that control the physical flow of gasoline.

This happened to occur at the same time as increases in COVID-19 vaccinations and car travel across the U.S. Because of this, the resulting gasoline shortage led to long lines at gas stations and high oil prices. That in turn directly affected consumers' wallets just as many were beginning to return to work and recover financially amidst a global pandemic.

This shows the importance of educating employees on data protection and data security best practices. In particular, make sure to use unique passwords for every account.

San Francisco Utility Fined $2.7 Million
The rise in smart meters introduces new threats to utilities such as power companies. One San Francisco-based utility was saddled with a $2.7 million fine from federal security regulators for failing to protect confidential data, which included more than 30,000 pieces of information. A third-party contractor allegedly copied data from the utility's network to its own. From there, it was hosted online without a user ID or password.

Threats of ransomware and denial-of-service attacks are also a concern for utilities that implement smart meters and store customer data on their network. That's a big problem if that network falls out of the control of the utility.

Solar Devices Create Portal to Access the Grid
Cyber attacks and big data security concerns affect all kinds of energy companies. In 2019, the Department of Energy reports, threat actors breached the web portal firewall of a solar power utility. This caused operators to lose visibility for parts of the grid for 10 hours.

Devices such as solar photovoltaic inverters that connect to the internet to help manage the grid can become targets. In particular, attackers can take advantage if the company doesn't update and secure their inverter software.

What Is the Cost of a Data Breach for Energy and Utilities Companies?
The Cost of a Data Breach Report, which has grown into a leading benchmark report in the cybersecurity industry, shares that the average cost of a data breach in the energy industry is $4.65 million. The good news is this figure has dropped by 27.2% since 2020 when the average cost of a data breach in the industry was up to $6.39 million.

Risks and Challenges of Data Security
Social engineering, system intrusion and web application attacks made up 98% of energy data breaches in 2021. Social engineering, or phishing, attacks were the most common, although ransomware attacks continue to be a threat for the sector.

According to the Verizon report, the following data was stolen, lost or rendered inaccessible by ransomware most often:

- Login credentials
- Internal company data

- Personal data of employees and customers.

In 98% of all cases, the threat actors were not connected with the companies in any way; only 2% of attacks were internal breaches.

There's more good news, too. The threat of 'hacktivism', threat actors who operate because of causes such as environmentalism and sustainability, is on a steep decline. According to the IBM X-Force Threat Intelligence Index, these attacks dropped by 95% between 2015 and 2019. Of course, oil and gas companies could be the primary targets of such attacks. So, their decline frees up energy cybersecurity departments to focus their budget and attention on other threats.

The rise of employees working from home and accessing networks remotely also creates a growing threat. The IBM report discovered that the cost of a data breach rose by an average of $1.07 million when remote work was a factor. In situations where more than 50% of the workforce was remote, it took IT security experts an average of 58 days longer to detect and contain threats.

Taking proactive steps toward employee education regarding cybersecurity best practices can help mitigate risks. Make sure your people know how to reduce the risk of compromised credentials, which were responsible for 20% of all attacks, according to the report. On top of that, train them to look out for the signs of social engineering and phishing.

Return to Top

HEADLINE	**11/02 Owner of huge leaked VPN database?**
SOURCE	**https://www.comparitech.com/blog/information-security/vpn-database-leak/**
GIST	More than 300 million records containing the personal information of VPN users was exposed on the web without a password, Comparitech researchers report. 45 million of the records included user account info such as email addresses, full names, and encrypted passwords. Based on our findings, ActMobile Networks Inc appears to be the owner of the data. The company operates Dash VPN, FreeVPN.org, and Dash Net Accelerated VPN, among others. However, ActMobile denied ownership of the data, saying it "does not maintain databases" in an email response to Comparitech. Comparitech's head of cybersecurity research, Bob Diachenko, discovered the exposed database on October 8, 2021 and immediately reported it to ActMobile in accordance with our responsible disclosure policy. The database was shut down a week later on October 15. The data has since been leaked on hacker forums, increasing users' risk of attack. The exposed data poses a serious risk to users whose personal information was exposed. The data could be used to launch phishing attacks and, if the passwords are compromised, account takeover and credential stuffing. The data could also be used to track VPN users by their devices' IP addresses. Comparitech has taken additional steps to verify the data's legitimacy and has confirmed that at least one user from the database did have an account with Dash VPN. **Timeline of the exposure** Here's what we know happened: • October 6, 2021 – The database was indexed by search engines. • October 8, 2021 – Diachenko discovered the exposed data and immediately alerted ActMobile per our responsible disclosure policy. The company did not respond to any of our attempts at contact to ActMobile support, team members, domain registrants, and server administrators. After multiple failed attempts to contact the company privately, Diachenko sent an alert on Twitter. • October 15, 2021 – The database was closed. • November 1, 2021 – The data was leaked on hacker forums.

The data was exposed for at least a week in total and has since been uploaded to hacker forums. Our honeypot experiments show attackers can find and steal unprotected data in a matter of hours, so users can assume the worst.

What data was exposed?
The MongoDB database was found at a France-based IP address and contained more than 100GB of data. That data can be divided up into three categories:

- 45 million user records, including…
  - Email address
  - Encrypted password
  - Full name
  - Username
  - Last login date
- 281 million user device info records, including…
  - IP address
  - Country code
  - Connection type (wi-fi or mobile)
  - Device and user ID
  - Accelerator ID
- 6 million purchase records, including…
  - Product purchased
  - Receipt

Additionally, more than 4 million "APN tokens" were exposed. We're not quite sure what these are, but they could be used for the **A**pple **P**ush **N**otification service, or they could be related to **A**ccess **P**oint **N**ames used to connect mobile devices to the internet over a cellular network.

No credit cards or other payment information were included.

Dangers of exposed data
Although the passwords were hashed and thus shouldn't be accessible, we advise anyone concerned users to immediately change their passwords. Any other accounts that share the same password should be changed as well to avoid credential stuffing. Enable two-factor authentication when possible.

Regardless of who is really responsible for the data, users should be on the lookout for targeted phishing messages purportedly from ActMobile, its brands, or related companies. Scammers might pose as one of these organizations to trick users into clicking a malicious link or download. Never click on unsolicited links or attachments.

Finally, we recommend VPN users who value their privacy choose a no-logs VPN. In particular, IP addresses collected by VPNs could be used to corroborate online activity and trace it back to an individual user. Comparitech recommends true zero-logs VPNs that don't collect your IP address or device identifiers, among other data.

Whose data is this?
ActMobile Networks' sole reply to Comparitech's multiple attempts at disclosure flat out denied ownership of the data, saying, "We do not maintain databases, so whatever is referenced is false. Furthermore, if you write about us we will take action."

But if the data doesn't belong to ActMobile, who does it belong to? Our findings don't support ActMobile's claim:

- The SSL certificate of the exposed server belonged to the actmobile.com domain.
- At least one user whose email was exposed confirmed they had an account with Dash VPN
- The exposed database repository containing most of the user information was labeled "Dashnet". There are several references in the database to ActMobile's VPN brands, such as in package names.

	• The WHOIS record for the IP address where the data was hosted lists ActMobile Networks as the owner If ActMobile is being honest about not owning the data, then someone must have tried very hard to make it seem as though ActMobile is responsible. US-based ActMobile Networks operates or white labels its VPN service to at least four VPN brands: FreeVPN.org, Dash VPN, Dash Net Accelerated VPN, and VPN Pro. Although the connection between these brands isn't immediately clear, clues in the database, their websites, and their app store pages hint at their relationship: • Dash VPN and Dashnet Accelerated VPN both share the same support email address. • DashVPN, Dashnet Accelerated VPN, and FreeVPN.org all list the same street address in Pleasanton, California as their headquarters. • The Amazon app store page for Dash VPN lists the FreeVPN.org email address, privacy policy, and website under its developer information. • Dashnet Accelerated VPN's website, listed on the Google Play store, leads to Dash VPN's website. Both FreeVPN.org and Dash Net Accelerated VPN have privacy policies that guarantee they do not collect any of the user's personal data when using the VPN. But as we can see above, they clearly collect users' IP addresses and device identifiers, so that claim wouldn't hold up in a Comparitech VPN review. Dash VPN does not have a privacy policy on its site, but its Amazon App store page points to the FreeVPN.org privacy policy. At time of writing, FreeVPN.org has a 4.3-star average rating and more than 1 million installs on Google Play. On the Apple Store, it is ranked #31 in the Utilities category with a 4.4-star rating. Dash VPN, also called Dash Office and VPN Dash (the branding is not consistent), has more than 500,000 installs and a 4.4 star review on Google Play. It has a 4.6-star rating on the Apple store. Dash Net Accelerated VPN has more than 50,000 installs on Google Play and a 3.7-star rating. It does not appear to be on the Apple App Store.
Return to Top	

HEADLINE	**11/02 Hoax: 'Groove' ransomware gang**
SOURCE	**https://krebsonsecurity.com/2021/11/the-groove-ransomware-gang-was-a-hoax/**
GIST	A number of publications in September warned about the emergence of "**Groove**," a new ransomware group that called on competing extortion gangs to unite in attacking U.S. government interests online. It now appears that Groove was all a big hoax designed to toy with security firms and journalists. Groove was first announced Aug. 22 on **RAMP**, a new and fairly exclusive Russian-language darknet cybercrime forum. "GROOVE is first and foremost an aggressive financially motivated criminal organization dealing in industrial espionage for about two years," wrote RAMP's administrator "Orange" in a post asking forum members to compete in a contest for designing a website for the new group. "Let's make it clear that we don't do anything without a reason, so at the end of the day, it's us who will benefit most from this contest." According to a report published by **McAfee**, Orange launched RAMP to appeal to ransomware-related threat actors who were ousted from major cybercrime forums for being too toxic, or to cybercriminals who complained of being short-changed or stiffed altogether by different ransomware affiliate programs. The report said RAMP was the product of a dispute between members of the **Babuk** ransomware gang, and that its members likely had connections to another ransomware group called **BlackMatter**.

"[McAfee] believes, with high confidence, that the Groove gang is a former affiliate or subgroup of the Babuk gang, who are willing to collaborate with other parties, as long as there is financial gain for them," the report said. "Thus, an affiliation with the BlackMatter gang is likely."

In the first week of September, Groove posted on its darknet blog nearly 500,000 login credentials for customers of **Fortinet VPN** products, usernames and passwords that could be used to remotely connect to vulnerable systems. Fortinet said the credentials were collected from systems that hadn't yet implemented a patch issued in May 2019.

Some security experts said the post of the Fortinet VPN usernames and passwords was aimed at drawing new affiliates to Groove. But it seems more likely the credentials were posted to garner the attention of security researchers and journalists.

Sometime in the last week, Groove's darknet blog disappeared. In a post on the Russian cybercrime forum **XSS**, an established cybercrook using the handle "**Boriselcin**" explained that Groove was little more than a pet project to screw with the media and security industry.

"For those who don't understand what's going on: I set up a fake Groove Gang and named myself a gang," Boriselcin wrote. The rest of the post reads:

"They ate it up, I dumped 500k old Fortinet [access credentials] that no one needed and they ate it up. I say that I am going to target the U.S. government sector and they eat it up. Few journalists realized that this was all a show, a fake, and a scam! And my respect goes out to those who figured it out. I don't even know what to do now with this blog with a ton of traffic. Maybe sell it? Now I just need to start writing [the article], but I can't start writing it without checking everything."

A review of Boriselcin's recent postings on XSS indicate he has been planning this scheme for several months. On Sept. 13, Boriselcin posted that "several topics are ripening," and that he intended to publish an article about duping the media and security firms.

"Manipulation of large information security companies and the media through a ransom blog," he wrote.

"It's so funny to read Twitter and the news these days But the result is great so far. Triggering the directors of information security companies. We f**k the supply chain of the information security office."

Throughout its short existence, Groove listed only a handful of victims on its darknet victim shaming blog, leading some to conclude the group wasn't much of a threat.

"I wouldn't take this call too seriously," tweeted The Record's **Catalin Cimpanu** in response to tweets about Groove's rallying cry to attack U.S. government interests. "Groove are low-tier actors with few skills."

Normally, when a cybercriminal forum or enterprise turns out to be fake or a scam, we learn the whole thing was a sting operation by federal investigators from the United States and/or other countries. Perhaps the main reason we don't see more scams like Boricelcin's is because there's not really any money in it.

But that's not to say his cynical ploy fails to serve a larger purpose. Over the past few years, we've seen multiple ransomware gangs reinvent themselves and rebrand to evade prosecution or economic sanctions. From that vantage point, anything which sows confusion and diverts the media and security industry's time and attention away from real threats is a net plus for the cybercriminal community.

Tom Hoffman, senior vice president of intelligence at Flashpoint, said mocking Western media outlets and reporters is a constant fixture of the conversation on top-tier cybercrime forums. "

"It is clear the criminal actors read all the press releases and Twitter claims about them," Hoffman said. "We know some of them just want to inflict pain on the West, so this type of trolling is likely to continue.

	With the high level of attention this one got, I would assume we will see some other copycats pretty soon." Cyber intelligence firm Intel471 said while it's possible that a single actor concocted Groove as a way to troll security researchers and the media, they believe it's more likely that the actor's attempt to create their own ransomware group didn't work out as they had planned. "It's also important to remember that the true identity and nature of any Ransomware-as-a-Service gang is not always clear and the membership makeup or affiliates of these gangs can be fluid," Intel 471 wrote. "Despite that and based on our research from multiple sources, which includes but isn't limited to observations of shared infrastructure and victimology, we believe "boriselcin" operated the Groove blog and the RAMP forum. This individual is a well-known member of the Russian-language cybercrime community with ties to a number of ransomware gangs and in August offered $1000 for someone to design a ransomware victim shaming blog for Groove. We are skeptical of the claims raised by the actor that Groove was an elaborate hoax from the beginning although we wouldn't be surprised to see further claims by the actor claiming this in future."
Return to Top	

HEADLINE	**11/03 Foreign tech firms pulling out of China**
SOURCE	**https://abcnews.go.com/Technology/wireStory/explainer-foreign-tech-firms-pulling-china-80942558**
GIST	HONG KONG -- Yahoo Inc. is leaving the China market, suspending its services there as of Monday amid what it says is an "increasingly challenging" business and legal environment. Foreign technology firms have been pulling out or downsizing their operations in mainland China as a strict data privacy law specifying how companies collect and store data takes effect. Such companies have decided the regulatory uncertainty and reputational risks outweigh the advantages of staying in the huge market. WHICH FOREIGN TECHNOLOGY COMPANIES HAVE RECENTLY DOWNSIZED OPERATIONS OR LEFT CHINA? Yahoo Inc. said in a statement Tuesday its services in China stopped as of Nov. 1. Users visiting the Engadget China site run by Yahoo this week find a popup notice saying the site will not publish any new content. Last month, Microsoft's professional networking platform LinkedIn said it would shutter the Chinese version of its site this year and replace it with a jobs board with no social networking functions. Epic Games, which operates the popular video game Fortnite, also says it will pull the game out of the China market as of Nov. 15. The game was launched in China via a partnership with the China's largest gaming company, Tencent, which owns a 40% stake in Epic. WHY ARE COMPANIES LEAVING CHINA NOW? The Personal Information Protection Law that took effect on Nov. 1 limits the amount of information companies are allowed to gather and sets standards for how it must be stored. Companies must get users' consent to collect, use or share data and provide ways for users to opt out of data-sharing. Companies also must get permission to send users' personal information abroad. The new law raises costs of compliance and adds to uncertainty for Western companies operating in China. Companies caught flouting the rules could be fined up to 50 million yuan ($7.8 million) or 5% of their yearly revenue.

Chinese regulators have cracked down on technology companies, seeking to curb their influence and address complaints that some companies misuse data and engage in other tactics that hurt consumers' interests.

The downsizing and departures also come as U.S. and China tussle over technology and trade. Washington has imposed restrictions on telecoms equipment giant Huawei and other Chinese tech companies, alleging they have ties with China's military and government.

Local companies are also feeling the heat, with e-commerce companies like Alibaba facing fines. Regulators are investigating some companies and have imposed strict rules that affect gaming firms like NetEase and Tencent.

WHAT OTHER HURDLES DO FOREIGN TECH COMPANIES FACE IN CHINA?

China operates what is known as a "Great Firewall" which uses laws and technologies to enforce censorship.

Content and keywords deemed politically sensitive or inappropriate must be scrubbed from the internet. Companies must police their own platforms, deleting posts and making sensitive keywords unsearchable.

Western social media networks such as Facebook and Twitter have long been blocked by the Great Firewall and are generally not accessible for people in mainland China.

"China has installed a very draconian policy governing internet operators, telling them what to do and especially what not to do," said Francis Lun, CEO of GEO Securities Limited in Hong Kong.

"I think the question comes down to why bother (operating as a foreign company in China) with such a limited return, and such heavy liability," he said.

Michael Norris, a research strategy manager at the Shanghai-based consultancy AgencyChina said compliance costs will rise further.

"Fortnite's exit is particularly damaging, as it shows not even a close partnership and investment with Tencent is enough to make the business case work," he said.

Foreign tech companies operating in China also face pressure from their home markets. Some U.S. lawmakers criticized LinkedIn's censorship of U.S. journalist profiles in China. In 2007, Yahoo Inc. was lambasted for handing over information on Chinese dissidents to the Chinese government that eventually led to their imprisonment.

WHAT DOES THIS MEAN FOR INTERNET USERS IN CHINA?

Chinese alternatives have popped up over the years to fill the void left by foreign social media platforms that have given up operating under the Great Firewall.

Instead of Google, China's most popular search engine is Baidu. Messaging apps like WeChat are used instead of WhatsApp or Messenger. Weibo, a microblogging platform, is the closest equivalent to Twitter, with more than 560 million Chinese users.

Unless they use a virtual private network (VPN) to mask their internet traffic and location and circumvent the web restrictions Chinese have fewer options for social networking and access to content and are likely to turn to strictly censored local alternatives.

Return to Top

Terror Conditions

Top of page

HEADLINE	11/04 Radicalization's path: cases similarities
SOURCE	https://apnews.com/article/business-religion-pakistan-media-social-media-ee6744ea3fa9c7adc5cf15ed058a75f5
GIST	In the months before he was charged with storming the Capitol, Doug Jensen was sharing conspiracy theories he'd consumed online. But it hadn't always been that way, says his brother, who recalls how he once posted the sort of family and vacation photos familiar to nearly all social media users. A world away, Wahab hadn't always spent his days immersed in jihadist teaching. The product of a wealthy Pakistani family and the youngest son of four, he was into cars and video games, had his own motorcycle, even studied in Japan. No two ideologues are identical. No two groups are comprised of monolithic clones. No single light switch marks the shift to radicalism. The gulf between different kinds of extremists — in religious and political convictions, in desired world orders, in how deeply they embrace violence in the name of their cause — is as wide as it is obvious. But to dwell only on the differences obscures the similarities, not only in how people absorb extremist ideology but also in how they feed off grievances and mobilize to action. For any American who casts violent extremism as a foreign problem, the Jan. 6 Capitol siege held up an uncomfortable mirror that showed the same conditions for fantastical thinking and politically motivated violence as any society. The Associated Press set out to examine the paths and mechanics of radicalization through case studies on two continents: a 20-year-old man rescued from a Taliban training camp on Afghanistan's border, and an Iowa man whose brother watched him fall sway to nonsensical conspiracy theories and ultimately play a visible role in the mob of Donald Trump loyalists that stormed the Capitol. Two places, two men, two very different stories as seen by two close relatives. But strip away the ideologies for a moment, says John Horgan, a researcher of violent extremism. Instead, look at the the psychological processes, the pathways, the roots, the experiences. "All of those things," Horgan says, "tend to look far more similar than they are different." THE AMERICAN America met Doug Jensen via a video that ricocheted across the Internet, turning an officer into a hero and laying bare the mob mentality inside the Capitol that day. Jensen is the man in a dark stocking cap, a black "Trust the Plan" shirt over a hooded sweatshirt, front and center in a crowd of rioters chasing Eugene Goodman, a Capitol Police officer, up two flights of stairs. One prominent picture shows him standing feet from an officer, arms spread wide, mouth agape. When it was all over, he'd tell the FBI that he was a "true believer" in QAnon, that he'd gone to Washington because Q and Trump had summoned "all patriots" and that he'd expected to see Vice President Mike Pence arrested. He'd say he pushed his way to the front of the crowd because he wanted "Q" to get the credit for what was about to happen. He'd tell his brother the photos were staged, how the police had practically let him in through the front door (prosecutors say he climbed a wall and entered through a broken window) and that some officers even did selfies with the crowd.

William Routh of Clarksville, Arkansas, had an unsettled feeling about that day even before the riot and says he cautioned his younger brother. “I said, if you go down there and you’re going to do a peaceful thing, then that’s fine. But I said keep your head down and don’t be doing something stupid.”

In interviews with the AP days and months after his younger brother’s arrest, Routh painted Jensen — a 42-year-old Des Moines father of three who’d worked as a union mason laborer — as a man who enjoyed a pleasant if unextraordinary American existence. He says he took his family to places like the Grand Canyon and Yellowstone National Park, attended his children’s sporting events, worked to pay for a son’s college education, made anodyne Facebook posts.

“I have friends that I speak to constantly that have conspiracy theories,” Routh said, “but this was a shock to me more than anything, because I would not have thought this from my brother Doug, because he’s a very good, hardworking family man and he has good values.”

Exactly who Jensen is, and how much knowledge he had of the world around him, depends on who’s talking.

A Justice Department memo that argued for Jensen’s detention cites a criminal history and his eagerness to drive more than 1,000 miles to “hear President Trump declare martial law,” then to take it into his own hands when no proclamation happened. It notes that when the FBI questioned him, he said he’d gone to Washington because “Q,” the movement’s amorphous voice, had forecast that the “storm” had arrived.

His lawyer, Christopher Davis, countered in his own filing by essentially offering Jensen up as a dupe, a “victim of numerous conspiracy theories” and a committed family man whose initial devotion to QAnon “was its stated mission to eliminate pedophiles from society.”

Six months after the insurrection, the argument resonated with a judge who agreed to release Jensen on house arrest as his case moved forward. The judge, Timothy Kelly, cited a video in which Jensen referred to the Capitol building as the White House and said he didn’t believe Jensen could have planned an attack in advance “when he had no basic understanding of where he even was that day.”

Yet less than two months after he was released, Jensen was ordered back to jail for violating the conditions of his freedom. Though barred from accessing a cellphone, he watched a symposium sponsored by MyPillow CEO Mike Lindell that offered up false theories that the presidential election’s outcome was changed by Chinese hackers. A federal officer making the first unannounced visit to Jensen found him in his garage using an iPhone to watch news from Rumble, a streaming platform popular with conservatives.

Davis, who weeks earlier had asserted that his client “feels deceived, recognizing that he bought into a pack of lies,” likened his client’s behavior this time to an addiction. The judge was unmoved.

“It’s now clear that he has not experienced a transformation and that he continues to seek out those conspiracy theories that led to his dangerous conduct on Jan. 6,” Kelly said. “I don’t see any reason to believe that he has had the wake-up call that he needs.”

Precisely when and how Jensen came to absorb the conspiracies that led him to the Capitol is bewildering to Routh, who says he took Jensen under his wing during a challenging childhood that included stays in foster care and now feels compelled, as his oldest living relative, to speak on his behalf.

When Jensen was questioned by the FBI, according to an agent’s testimony, he said for the last couple of years he’d return home from an eight-hour workday and consume information from QAnon. In the four months before the riot, the brothers communicated about QAnon as Jensen shared videos and other conspiracy-laden messages that he purported to find meaning in but that Routh found suspect.

It was a period rife with baseless theories, advanced on the Internet and mainstream television, that an election conducted legitimately was somehow stolen in favor of Democrat Joe Biden. “It was just out there. It is on the internet everywhere,” Routh says.

Routh, who says he's a Republican who supported Trump, maintains his brother and others like him were frightened by the prospect of a Biden victory. Before Jan. 6, Routh says, "We have been being told for the last — what? — seven, eight months that if the Democrats get control, we're losing our country, OK? That scares a lot of people."

He says he understands the anxiety of Trump supporters who fear the country may get more radical on the left. He has friends in oil fields and the pipeline industry who don't know "if they're going to be able to feed their families again." As Routh criss-crossed the country as a truck driver, he says the idea Trump would lose re-election seemed unfathomable given that virtually everyone he met, everywhere he went, was pushing "Trump, Trump, Trump."

When Routh looks at the photos of Jensen and the group he was with Jan. 6, he doesn't see a determination to physically hurt anyone or vandalize the building. And despite the QAnon T-shirt, and despite the statement to the FBI that he was "all about a revolution," Routh insists his brother was more a follower than a leader. Jensen is not among those charged with conspiracy or with being part of a militia group, and though prosecutors say he had a pocket knife with him, his lawyer says it was from work and he never took it out.

"He had a lot of influence from everybody else there," Routh said this summer as he awaited a judge's ruling on his brother's bond motion. "And he has always been the kind of kid that says, 'I can do that.'"

Two days after the riot, back home in Iowa, Jensen walked 6 miles (9.66 kilometers) to the Des Moines police department after seeing he was featured in videos of the chaos, an FBI agent would later testify. There, the FBI says, he made statements now at the center of the case, including admitting chasing Goodman up the stairs, that he yelled "Hit me. I'll take it" as the officer raised a baton to move him back and that he profanely bellowed for the arrests of government leaders.

Though prosecutors suggest he had the presence of mind to delete potentially incriminating social media accounts from his phone, he also seemed uncertain — confused, even — during his encounter with law enforcement. As officials questioned him, according to an FBI agent's testimony, he said words to the effect of, "Am I being duped?"

THE PAKISTANI

Wahab had it all. The youngest son of four from a wealthy Pakistani family, he spent his early years in the United Arab Emirates and for a time in Japan, studying. Wahab liked cars, had his own motorcycle and was crazy about video games.

His uncle, who rescued the 20-year-old from a Taliban training camp on Pakistan's border with Afghanistan earlier this year, asked that his full name not be used because in the northwest where the family lives, militants have deep-reaching tentacles. But more than that, he worries about his family's reputation because of its prominence. He agreed to be quoted using his middle name, Kamal.

The family has business interests scattered across the globe. Kamal is one of five brothers who runs the family-owned import/export conglomerate. Each brother in turn has groomed and primed their sons for the business. Wahab's older brothers are already running overseas branches of the family business.

Wahab's future was to be no different. He returned to Pakistan in his early teens from abroad. Being the youngest son in a society that prizes males, he was spoiled. His older brothers sent him "pocket money," his uncle said. Other than school, Wahab had few responsibilities.

His uncle blamed his slide to radicalization on the neighborhood teens Wahab hung out with in their northwest Pakistan hometown — not to mention video games and Internet sites.

Wahab's friends introduced him to dozens of sites, his uncle said. They told of Muslims being attacked, women raped, babies brutally killed. The gruesomeness was horrifying, though Kamal says there was no way to know what was true — or if any had been doctored. But for Wahab, the images were deeply disturbing.

"He felt like he hadn't known what was going on, that he had spent his life in darkness and he felt he should be involved. His friends insisted he should. They told him he was rich and should help our people," his uncle said.

To his uncle, Wahab seemed to become increasingly aggressive and fixated on violence with the seemingly endless hours he spent playing video games. One in particular, called PUBG, was all the rage with Wahab and his friends.

"All the boys loved it," Kamal said. "For hours they would play as a team against the computer."

On pubgmobile.com, the game is described as focusing "on visual quality, maps, shooting experience ... providing an all-rounded surreal Battle Royale experience to players. A hundred players will land on the battleground to begin an intense yet fun journey." Wahab's uncle said he'd be shouting instructions as he played, interacting with teammates.

Suddenly, earlier this year, Wahab disappeared. His parents, frantic, searched everywhere. Wahab wasn't the first in the family to flirt with extremism. His cousin Salman had joined the local Pakistani Taliban years before. But he was different: He'd never been interested in school and was sent to a religious school, or madrassa, for his education. The family had long given up on him.

Salman swore he hadn't seen Wahab and knew nothing of where he might be — or if he had even joined jihad.

Suspicion then fell on Wahab's friends. Family members were certain they'd induced him to defend against attacks that Wahab and his friends were convinced were being waged against Muslims, simply because of their religion.

The family used its influence and money to press the fathers of Wahab's friends to find the 20-year-old. They finally located him at a Pakistani Taliban training camp, where Kamal said Wahab was being instructed in the use of small weapons.

Such camps are also often used to identify would-be suicide bombers and instruct them in the use of explosives, identification of soft targets and how to cause the greatest destruction. The Pakistan Taliban have carried out horrific attacks; in 2014, insurgents armed with automatic rifles attacked a public school, killing more than 150 people, most children, some as young as 5.

When Wahab's father discovered his son was at a training camp, he was furious, said his uncle.

"He told the people, 'Leave him there. I don't accept him as my son anymore.' But I took it on myself to bring him back," Kamal said. He said he didn't ask Wahab about the camp or why he wanted to go — or even such basics as how he got there.

"I didn't want him talking about any of it. I didn't want to know why he went because then I knew he would start to get excited again and he would start thinking about it all over again," Kamal said. "Instead, I took a firm face with him."

His uncle told Wahab he was getting another chance — his last.

"I told him, 'Now it is on me. I have taken the responsibility. You won't get another chance. If you do anything again then I will shoot you,'" his uncle said. In Pakistan's northwest, where tribal laws and customs often decide family disputes and feuds, the threat was most likely not an idle one.

Today, Wahab is back in the family business, but his uncle says he is closely watched. He isn't allowed to deal with the company finances and his circle of friends is monitored. "Right now we don't trust him. It will take us time," his uncle says.

Fearful that others among Wahab's siblings and cousins could be enticed to extremism, the family has imposed greater restrictions on young male relatives. Their independence has been restricted, Kamal says: "We are watching all the young boys now, and most nights they have to be home — unless they tell us where they are."

—

Moral outrage. A sense of injustice. A feeling that things can only be fixed through urgent, potentially violent action.

Those tend to motivate people who gravitate toward extremism, according to Horgan, who directs the Violent Extremism Research Group at Georgia State University. He says such action is often seen as necessary to ward off a perceived impending threat to one's way of life — and to secure a better future.

"Those similarities you will find repeated across the board, whether you're talking about extreme right-wing militias in Oklahoma or you're talking about a Taliban offshoot in northwest Pakistan," Horgan says.

The world views driving extremist groups may feel fantastical and outrageous to society at large. But the true believers who consume propaganda and align themselves with like-minded associates don't see it that way. To them, they possess inside knowledge that others simply don't see.

"There's a contradiction, because they are committed insiders but part of their insider status is defined by pitting themselves against an outsider whose very existence is said to threaten their own," Horgan says. "They pride themselves on being anti-authoritarian. Yet conformity is what binds them together."

Research shows that people who espouse conspiracy theories tend to do poorer on measures of critical thinking. They reduce complex world problems — the pandemic, for instance — to simplified and reassuring answers, says Ziv Cohen, a forensic psychiatrist and expert on extremist beliefs at Weill Cornell Medical College of Cornell University.

Rather than attributing a job loss to the effects of globalization, for instance, one might see it as the result of a conspiracy that someone in particular has engineered.

"It gives us answers," he says, "that are much more appealing emotionally than the real answer."

That's where the stories of Jensen and Wahab seem to intersect. Both were seeking something. Both found answers that were enticing, attractive — and distorted versions of reality.

"For reasons he does not even understand today, he became a 'true believer' and was convinced he (was) doing a noble service by becoming a digital soldier for 'Q,'" Davis, Jensen's lawyer, wrote in a June court filing. "Maybe it was mid-life crisis, the pandemic, or perhaps the message just seemed to elevate him from his ordinary life to an exalted status with an honorable goal."

But is that goal ever reached? Is comfort ever found? Oddly, and perhaps counterintuitively, research has shown that when extremists' conspiracy theories are reinforced, their anxiety levels rise rather than fall, Cohen says. He likens the comfort to a drug — one that requires increasingly more consumption to take effect. Which helps perpetuate the cycle.

Says Cohen: "People seem to not be able to get enough of a conspiracy theory, but they're never quite satisfied or really reassured."

Return to Top

HEADLINE	**11/03 Calif. man jailed 25yrs: bombing plot**
SOURCE	https://www.oc-breeze.com/2021/11/03/204877_san-fernando-valley-man-who-plotted-the-bombing-of-long-beach-rally-sentenced-to-25-years-in-federal-prison/
GIST	A San Fernando Valley man who planned the bombing of a political rally in Long Beach in 2019 was sentenced to 25 years in federal prison. Mark Steven Domingo, 28, of Reseda, was sentenced by United States District Judge Stephen V. Wilson. At the conclusion of a five-day trial, a federal jury on August 11 found Domingo guilty of one count of providing material support to terrorists and one count of attempted use of a weapon of mass destruction. Judge Wilson sentenced Domingo to 15 years' imprisonment on the providing material support count and 25 years in federal prison for attempted use of a weapon of mass destruction – both sentences to be served concurrently. The court also ordered Domingo to be placed on supervised release for a term of 20 years once Domingo completes his prison sentence. Domingo has been in federal custody since his arrest in April 2019. "This defendant planned a mass-casualty terrorist attack and repeatedly admitted at trial that he had a desire to kill as many people as possible," said Acting United States Attorney Tracy L. Wilkison. "Had this bombing been successful, many innocent people would have been murdered, yet this defendant has shown no remorse for his conduct, nor has he renounced the extremist ideology that motivated his horrific plot." "Mr. Domingo represents the very real threat posed by homegrown violent extremists in the United States," said Kristi K. Johnson, the Assistant Director in Charge of the FBI's Los Angeles Field Office. "Domingo's plans and a potentially catastrophic attack were thwarted when the Joint Terrorism Task Force learned of his intentions in advance and carried out this successful undercover operation with our partners. This case was the result of a collaborative effort with the Naval Criminal Investigative Service, the Los Angeles Police Department, the Los Angeles County Sheriff's Department, and the Long Beach Police Department." The investigation into Domingo was prompted by his online posts and conversations in an online forum in which he expressed support for violence, specifically a desire to seek violent retribution for attacks against Muslims, as well as a willingness to become a martyr. After considering various attacks – including targeting Jewish people, churches, and police officers – Domingo decided to bomb a rally scheduled to take place in Long Beach in April 2019. As part of the plot, Domingo asked a confederate – who actually was working with the FBI as part of the investigation – to invite a bomb-maker into the scheme. Domingo then purchased and provided to the confederate and the bomb-maker – who in fact was an undercover law enforcement officer – several hundred 3½-inch nails to be used as shrapnel for the bombs. Domingo specifically chose those nails because they were long enough to penetrate organs in the human body. Leading up to the attack, Domingo called for an event similar to the October 2017 mass shooting in Las Vegas. Following an attack on Muslims in New Zealand in March 2019, Domingo called for retribution in an online post. Domingo selected the Long Beach rally as his target and, in April 2019, drove his confederate and the undercover officer to Long Beach to scout the location he planned to attack. While there, Domingo discussed finding the most crowded areas to place the bombs so he could kill the most people. On April 26, 2019, Domingo received what he thought were two live bombs, but actually were inert explosive devices delivered by an undercover law enforcement officer. He was arrested that same day with one of the bombs in his hands.

	"At trial, [Domingo] testified and repeatedly affirmed that he intended to commit mass murder in March and April 2019," prosecutors wrote in a sentencing memorandum that recommended a sentence of life in prison. "He admitted that the [confidential informant] stopped him from committing at least one murder in April 2019 by encouraging him to be patient. Finally, he admitted that he was excited when he learned that the [confidential informant] had access to an individual who could construct a bomb, and that he was the one who chose to attack the rally, chose to use the bombs, and chose to go through with the plot to commit mass murder, right up until the moment of his arrest." The FBI's Joint Terrorism Task Force (JTTF) investigated this matter. JTTF members who participated in the investigation include the FBI, the Los Angeles Police Department, the Naval Criminal Investigative Service, the Los Angeles County Sheriff's Department and the Long Beach Police Department. Assistant United States Attorneys Reema M. El-Amamy and David T. Ryan of the Terrorism and Export Crimes Section, along with Trial Attorneys Lauren Goddard and Joshua Champagne of the National Security Section's Counterterrorism Section at the Department of Justice, prosecuted this case.
Return to Top	

HEADLINE	**11/03 EU terrorism training Mozambique troops**
SOURCE	**https://africa.cgtn.com/2021/11/04/eu-mission-to-train-mozambican-troops-to-fight-terrorism/**
GIST	The European Union launched a military mission Wednesday to train Mozambican troops to fight terrorism in the country's northern province of Cabo Delgado. Inaugurated in the capital Maputo, the mission is meant to provide specialized training for two years in combating terrorism and protecting civilians, said its commander, Brigadier General Nuno Lemos Pires of the Portuguese army. The mission will have 140 training officers divided between two training centers — one for commandos in Chimoio in central Mozambique and the other for marines in the country's capital Maputo. It will contribute to improving the security situation in the country, said Mozambican Defense Minister Jaime Neto, while Portugal's National Defense Minister Joao Cravinho said the training would offer an example of effectiveness in the eyes of Mozambicans. An armed insurgency with its origins in the wider socio-economic and political disparity has kept Mozambique smoldering since 2017. Terrorist activities and insurgency in northern Mozambique have left more than 3,000 people dead and nearly 800,000 displaced, according to official data. In July, Rwanda deployed 1,000 army and police personnel to Mozambique's restive province of Cabo Delgado to help combat terrorism. The Southern African Development Community (SADC) has also deployed a military force to Mozambique to help the government combat terrorism and acts of violent extremism.
Return to Top	

HEADLINE	**11/04 Taliban leader: infiltrators within ranks**
SOURCE	**https://www.france24.com/en/live-news/20211104-taliban-leader-warns-against-infiltrators-in-the-ranks**
GIST	Kabul (AFP) – The supreme leader of the Taliban warned Thursday against the danger of turncoats and infiltrators in the movement that has taken charge of Afghanistan. Reflecting the seriousness of the threat, the reclusive Haibatullah Akhundzada issued a rare written public statement to urge Taliban commanders to purge their ranks.

	In it he says "all those elders of their groups must look inside their ranks and see if there is any unknown entity working against the will of the government, which must be eradicated as soon as possible. "Whatever wrong happens, the elder will be responsible for the consequences of the actions in this world and in the afterlife," he warned, in a statement tweeted out by multiple Taliban accounts. The Islamist militant movement seized power in August after overrunning the capital and ousting the collapsing US-backed government, declaring a new Islamic Emirate of Afghanistan. But after 20-years of guerrilla warfare, the Taliban has been forced to expand their ranks rapidly by recruiting former foes, allied Islamist militants and young madrassa students. Now that it is the government, the movement faces attacks in its turn from hardline factions like the Islamic State-Khorasan (IS-K). The groups are now bitter rivals, but there has been movement between them over the years and they both employed tactics like suicide bombings and civilian massacres to destabilise the former regime. On Tuesday, at least 19 people including a Taliban commander were killed in a gun and suicide bomb attack claimed by IS-K on a military hospital in the heart of Kabul. Taliban commanders insist that they can re-establish stability and security, but there have also been killings blamed on Taliban elements or extremist infiltrators. Last week, for example, gunmen who presented themselves as Taliban shot dead three wedding guests in a dispute about the playing of music, which the movement frowns upon. Taliban spokesman insisted the killers were not acting under orders and promised they would be punished. In his statement, Akhundzada said Taliban unit commanders must take the time to sit down with their recruits to "try to work on their manners and behaviour so that these mujahideen can work better for his leader."
Return to Top	

HEADLINE	**11/03 IS stepping up attacks east, central Syria**
SOURCE	**https://www.voanews.com/a/islamic-state-militants-stepping-up-attacks-in-eastern-central-syria-/6298777.html**
GIST	According to local reports, militants linked to the Islamic State terror group have stepped up their attacks in eastern and central Syria in recent days. The local North Press Agency reports that at least two Syrian government soldiers were killed Monday in an attack carried out by suspected IS fighters near the ancient town of Palmyra in central Syria. The militants reportedly targeted a checkpoint guarded by Syrian army soldiers from the 4th Division, concealing themselves behind a seized military vehicle. Local news reports say at least seven Syrian government soldiers and Iranian-backed militiamen were killed two days prior in two separate IS attacks in eastern Syria. IS militants continue to undertake massive attacks against their opponents in Syria and Iraq, despite losing nearly all of the land they once controlled. The group has been particularly active in Syria's Badia desert, which is controlled by government forces, Iranian- and Russian-backed militias in central Syria. Russia and Iran are two main supporters of Syrian President Bashar al-Assad's government.

	"The Badia is a very interesting area in Syria right now," said Rami Abdulrahman, director of the Britain-based Syrian Observatory for Human Rights. "It connects regime-held areas to those controlled by Turkish-backed groups in parts of northern and western Syria," he told VOA. "And so [IS] militants can roam between the two areas and manage to avoid Russian airstrikes." In response to increasing IS activity in the area, Russian planes on Monday carried out at least 15 airstrikes against hideouts believed to belong to the militants, according to the Syrian Observatory. Omar Abu Layla heads Deir Azzour 24, a journalism and research group focused on developments in eastern Syria. Abu Layla says the current acceleration of IS strikes is a result of two factors. "The first one is merely an attempt to boost the morale of its fighters and to show its supporters that the group is still capable of conducting deadly operations against any opposing force," he told VOA. The other factor, Abu Layla said, is "that they try to end the nearly absolute sway of Iranian forces on the military supply line that stretches from the Iraqi border all the way to Shayrat airbase in Homs province and other areas in Syria." IS also has active cells in some areas under the control of the U.S.-backed Syrian Democratic Forces (SDF) in eastern Syria, particularly in Deir el-Zour province. In October, 21 anti-IS operations were carried out by the SDF, the group said Monday. The operations, supported by the U.S.-led coalition troops, resulted in the arrest of 51 IS suspects, also known as Daesh. "These joint operations demonstrate our mutual commitment as partners to deny Daesh any presence to influence in Northeast Syria," the coalition said on Twitter.
Return to Top	

HEADLINE	**11/03 FBI declassifies 9/11 documents**
SOURCE	**https://www.wwnytv.com/2021/11/03/fbi-releases-declassified-documents-sept-11-attacks/**
GIST	WASHINGTON (AP) — The FBI released hundreds of pages of newly declassified documents Wednesday about its long effort to explore connections between the Saudi government and the Sept. 11 attacks, revealing the scope of a strenuous but ultimately fruitless investigation whose outcome many question to this day. Agents for years investigated support given to several of the hijackers upon their arrival in the U.S., focusing in particular on whether three Saudi nationals — including a Saudi Embassy official in Washington — had advance knowledge of the attacks. Ultimately, investigators found insufficient evidence to charge any of the three with illegally supporting the hijackers, according to an FBI memo from May that closed out the probe and was among the more than 700 pages released Wednesday. The FBI noted in the memo that al-Qaida compartmentalized the roles within its major attacks and “did not make the attack plans known in advance to others” for fear of word getting out. “Specifically, in relation to the 9/11 attacks, the hijackers knew there was a martyrdom operation, but did not know about the nature of the operation until shortly before the attack for operational security reasons,” the FBI memo states. The documents were the latest materials to be released under an executive order from President Joe Biden aimed at making public long-classified investigative reports related to the attacks. A separate investigative document was released on the 20th anniversary of the attacks in September. The records have long been sought by victims’ relatives as they sue in federal court in New York to try to prove that the Saudi government was complicit, something Riyadh officials have vigorously denied.

The Saudi Embassy in Washington did not respond to a request for comment Wednesday, but issued a statement in September calling any allegations of complicity malicious and categorically false.

U.S. government investigations over the past two decades have documented support given by Saudi government officials to several of the hijackers upon their arrival in the U.S., but have not produced clear evidence that senior government leaders helped plot the attacks. The FBI memo closing out the investigation says the bureau "has not identified additional groups or individuals responsible for the attack other than those currently charged."

Even so, the documents reveal new details about the years-long efforts by the FBI to hunt for possible involvement by the Saudi government and to scrutinize support given by Saudi nationals in the U.S. to the first two hijackers to arrive in the U.S., Nawaf al-Hazmi and Khalid al-Mihdhar.

Andrew Maloney, a lead lawyer for the victims' families, said the FBI has "now released a substantial amount of very incriminating documents regarding the Saudi government's role in helping al-Qaida and these two hijackers in particular."

Brett Eagleson, whose father, Bruce, died in the World Trade Center attack, said in a statement that the details in the documents "help bolster the arguments that high-level Saudi officials aided and supported the 9/11 hijackers."

Among the episodes scrutinized by the FBI and recounted in the records is a February 2000 encounter at a Southern California halal restaurant between al-Hazmi and al-Mihdhar and a Saudi national named Omar al-Bayoumi, who subsequently helped them lease an apartment in San Diego. He had previously drawn FBI scrutiny but was never charged over his connections with the future hijackers.

According to the records released Wednesday, the FBI also investigated ties between al-Hazmi and al-Mihdhar and people linked to the Saudi Ministry of Islamic Affairs, which funds mosques and efforts to promote Islam around the world.

According to one of the documents, the FBI studied whether al-Qaida operatives had "infiltrated" the ministry unbeknownst to the Saudi government or whether there was a "collaboration of AQ operatives and certain radical elements within the Ministry of Islamic Affairs for mutually beneficial goals."

The FBI examined whether Saudis who had given financial support to al-Hazmi and al-Mihdhar had ties to the plotters of the attack.

According to the documents, al-Bayoumi was in contact with Musaed al-Jarrah, who served as director of Islamic affairs at the Saudi Embassy in Washington and who the FBI suspected "may have been trying" to bring extremists into the U.S. using his embassy position. In its final summary of the investigation, the FBI described al-Jarrah as a "controlling, guiding, and directing influence on all aspects of Sunni extremist activity in Southern California."

Maloney, the plaintiffs' lawyer, said those allegations are significant.

"Here we now have for the first time the FBI telling the world that Jarrah was an extremist, and he was bringing in Sunni extremist imams into the United States and then supervising them," he said.

But authorities had insufficient evidence that al-Jarrah, al-Bayoumi and a third man — Fahad al-Thumairy, who was an accredited diplomat at the Saudi Consulate in Los Angeles and who investigators say led an extremist faction at his mosque — had conspired to assist the hijackers.

None of the three was charged, and all have since left the country, the FBI said.

	The Trump administration fought to keep al-Jarrah's identity private before the Justice Department accidentally released it last year in a court filing. In a Sept. 8, 2021, memo, the FBI corrected a previous assertion it made and said there was no evidence to prove that al-Jarrah had any personal contact directly with the two hijackers who were the focus of the investigation. The documents also show investigators repeatedly re-interviewed Mohdar Abdullah, a Yemeni student who befriended al-Hazmi and al-Mihdhar when they settled in San Diego. He was arrested after the attacks as a suspected material witness, an allegation he has denied. After nearly three years in custody, he was deported to Yemen in 2004. Abdullah has told investigators that he believed Saudi officials may have been complicit in the Sept. 11 plot by helping the hijackers settle in Southern California. But he could not provide agents with evidence. "When questioned why he believes that, Abdullah stated that is his opinion and he doesn't know anything more than what he provided to the FBI in the past," the documents say.
Return to Top	

HEADLINE	**11/03 FBI: equal threats domestic extremists, IS**
SOURCE	**https://www.reuters.com/world/us/fbi-believes-us-faces-equal-threats-domestic-extremists-islamic-state-official-2021-11-03/**
GIST	WASHINGTON, Nov 3 (Reuters) - U.S. law enforcement and security agencies believe domestic extremists, notably white supremacists, pose a violent threat in the United States similar to that of Islamic State militants, top U.S. security officials told Congress on Wednesday. Concern about racially motivated domestic extremists had prompted the FBI to elevate the threat to a level equal with that posed by the Islamist militants, said Timothy Langan, the assistant director who heads the counterintelligence division. Langan told a House Intelligence subcommittee the Federal Bureau of Investigation had detected a significant increase in the threat of violence from domestic extremists over the last 18 months. He said the bureau was conducting around 2,700 investigations related to domestic violent extremism, and there had been 18 lethal attacks targeting U.S. religious institutions in which 70 people had died in recent years. The FBI has engaged with tech companies regarding their role in fueling extremism, has successfully disrupted planned acts of violence and will continue to "try to close the gap" on its inability to legally decode encryptions on mobile phones. John Cohen, acting undersecretary for Intelligence and Analysis in the Department of Homeland Security, told the subcommittee that racial superiority and "hatred of immigrants" were major threat concerns. He said his department believes the biggest domestic threat is posed by lone offenders and small groups indoctrinated in extremist ideology. The threat is fueled by a blend of extremist beliefs and personal grievances, he said. Cohen noted that domestic extremists conduct so much discussion openly on social media that covert collection of intelligence on the threats they pose may often not be necessary to spot the threats. Some Republican members of the House subcommittee suggested U.S. spy agencies should not be collecting information on U.S. political activity unless there is a connection to foreign actors.
Return to Top	

HEADLINE	**11/03 AQ doubles down hatred on Jews, Israel**
SOURCE	**https://www.homelandsecuritynewswire.com/dr20211103-in-9-11-video-al-qaeda-doubles-down-on-enmity-toward-jews-and-israel**
GIST	Each year, to commemorate the September 11, 2001 terrorist attacks on the United States, the notorious terrorist group Al Qaeda releases a video featuring one of the group's senior leaders who typically reiterates the significance and impact of those deadly events from their warped perspective. Al Qaeda's 2021 video, which was recently analyzed by experts in ADL's Center on Extremism and the ADL department of International Affairs, was notable for several reasons. First, it contains minimal footage of 9/11 itself, a departure from the typical emphasis on the violence of that day. Second, the video prominently features leader Ayman al Zawahiri, who many Western analysts speculated had died, focusing explicitly on Israel. Zawahiri introduced the film as part of Al Qaeda's "Jerusalem will not be Judaized" campaign, which was launched after the December 2017 announcement by the Trump Administration that it was planning to move the U.S. embassy from Tel Aviv to Jerusalem. The video provides crucial context for the group's extremist agenda, underscoring that Al Qaeda is particularly focused on a strike against Israel, and that anti-Semitism remains an animating element of Al Qaeda's worldview. **Al Qaeda's Intention to Target Israel** Typically, the 9/11 anniversary is a major propaganda opportunity for Al Qaeda's central leadership, so the decision to replace its typical messaging with content focusing unambiguously on Israel was itself remarkable. In the video, Zawahiri spends a significant amount of time laying out a timeline of the creation of Israel, starting with the period of Western military control of the Middle East after World War I. He frames the narrative to suggest that Arab leaders were initially manipulated and lied to by the European powers to force them to acquiesce to the establishment of the state of Israel. Zawahiri reserves particular vitriol for Arab leaders for failing to be tougher against Israel, particularly those who pursued peace accords with the country. The viciousness of Zawahiri's criticism for Arab leaders who have established diplomatic relations with Israel is part of a longstanding theme in Al Qaeda propaganda, likely exacerbated in this instance by the success of the 2020 Abraham Accords, which demonstrates that opposition to Israel is no longer a political necessity for some leaders in the region. This also weakens the standing of hardliners like Al Qaeda, since it undermines the claim that violence is the only solution to the Arab-Israeli conflict. Zawahiri closes the video with a reference to Abdullah Azzam, an extremist who is considered the founding father of the modern jihadist movement. The video shows a clip from a famous Azzam speech in which he argues that jihad is a global movement and that although the path of jihad will ultimately lead to Palestine, it must first pass through Afghanistan. Zawahiri's language throughout the video underscores that attacking the West and Israel remain a top priority for Al Qaeda, even if many of its forces or activities are elsewhere, in places such as Afghanistan. Given Al Qaeda's recent gains in Afghanistan thanks to the Taliban's takeover, this possible emphasis on Afghanistan as a staging ground for attacking Israel is especially worrying. The fact that Al Qaeda released a video centered on Israel to commemorate its 9/11 attacks signals the group's commitment to targeting the country in the future. Over the past few months, Al Qaeda's other propaganda outlets have also directed increased attention towards Israel, suggesting that as the group builds capacity, this may be a major target for future attacks. **Al Qaeda's Inherent Anti-Semitism** Al Qaeda's decision to focus on Israel on the 20th anniversary of its most notorious terrorist attack also revealed the extent to which anti-Semitism animates the group's larger worldview and ideology. This is not a new development. In the aftermath of 9/11, the U.S. government's bipartisan 9/11 Commission Report documented numerous instances in which the hijackers and Al Qaeda's senior

leadership were influenced by antisemitic hate and conspiracy theories. As that report noted, Al Qaeda's own operatives were speaking in terms of waging war against "Jews and Crusaders" and lashing out at "a global movement centered in New York City that supposedly controlled the financial world and media."

The organization's 9/11 anniversary propaganda video is a stark reminder that such anti-Jewish bigotry remains a major part of the group's narrative today.

Al Qaeda's 9/11 anniversary video urges followers to join in its terrorist activities, describes Israel as essentially a military base for Western interests, and argues that attacking Israel also directly harms Western powers in general and the U.S. in particular. The video entreats viewers, "Participate," and asks, "can you be satisfied with your lives… while you witness daily live broadcasts of the crimes of the Jews in Palestine," which it called "the focal cause of the Muslim Ummah [world]."

The video claims that Palestine is "in the hands of monkeys and swines for over a century… the Jews," and that "only when actions match words" will Muslims be able to achieve "the liberation of al Aqsa from the clutches of the Jews."

However, in order to achieve this goal, Zawahiri explains in the video that "the battle must be taken beyond this besieged strip. Just as they have come together from all corners of the world to fight us, we must hit them hard everywhere." He focuses particularly on Arab leaders over the years whom he considers insufficiently hostile to Israel and are therefore portrayed as treacherous co-conspirators in the service of Zionists. In this same vein, a senior leader from Al Qaeda's Yemeni branch asks, "Do you accept sitting back while you watch treacherous rulers collaborating to strike deals of disgrace, submission and normalization with the Jews, beginning from Camp David, all the way to Oslo and finally the Deal of the Century?"

The video condemns leaders of the Palestine Liberation Organization for permitting "contacts with Jewish powers" since the 1970s. It calls contemporary Palestinian leaders such as Mahmoud Abbas and Mohammad Dahlan "the biggest broker," "the son of Satan," and "secular heretics fostered and financed by America and Israel so as to uproot Islam." It calls the late Egyptian President Anwar Sadat "Anwar al-Yahood," meaning "Anwar of the Jews" for signing a "treaty of surrender" with Israel. And it calls the UAE's de facto ruler Mohammed bin Zayed Al Nahyan "the puppet, the midget, the leader of mercenary militias," along with deriding Sudan's top military official as "the paid mercenary, Burhan of Sudan." The fact that Zawahiri dedicates such a large portion of the video to directing hatred at Arab leaders is reflective of the realities of Al Qaeda's strategy; the majority of Al Qaeda's victims are not the Westerners they profess to target, but rather Muslim civilians.

Yet Zawahiri advises the listener that these Arab leaders are not Al Qaeda's main concern. Instead, he proclaims that "we should not be surprised by the treachery and negligence of the betrayers" and that "the matter is far more serious. It is a Crusade led by America, and Israel is one of the most important tools of this Crusade. Israel is a Crusader fortress, equipped with nuclear weapons in the heart of the Islamic world."

Such calls to target Israel, the United States and America's Arab allies are nothing new in Al Qaeda's propaganda or approach in practice. Yet the organization's video marking 20 years since 9/11 provides yet another reminder that Al Qaeda remains a deeply antisemitic organization that seeks to attack Israel, Jews and their purported "lackeys" with terrorist activities and propaganda.

Return to Top

HEADLINE	**11/03 Investigation into 'mistake' 29 Aug airstrike**
SOURCE	**https://www.nytimes.com/2021/11/03/us/politics/drone-strike-kabul-child.html**
GIST	WASHINGTON — Surveillance videos showed the presence of at least one child in the area some two minutes before the military launched a drone strike on a site in Kabul, Afghanistan, in August, the Defense Department said on Wednesday.

But the general who conducted the investigation into the U.S. airstrike, which the military has acknowledged mistakenly killed 10 civilians, including seven children, said the footage showing the presence of a child would have been easy to miss in real time.

The inquiry by the Air Force's inspector general, Lt. Gen. Sami D. Said, found no violations of law and does not recommend any disciplinary action. The general blamed a series of assumptions, made over the course of eight hours as U.S. officials tracked a white Toyota Corolla through Kabul, for causing what he called "confirmation bias," leading to the Aug. 29 strike.

"That assessment was primarily driven by interpretation," the general said on Wednesday during an unclassified briefing on the report to news media at the Pentagon. "Regrettably, the interpretational assessment was inaccurate."

While General Said acknowledged that the military had video footage showing a child at the site two minutes before the launch, he said that he was unsure whether anyone who was not specifically looking for evidence of a child would have picked up on it.

"Two independent reviews that I conducted, the physical evidence of a child was apparent at the 2-minute point," he said. "But it is 100 percent not obvious; you have to be looking for it."

The military makes an effort to avoid civilian casualties. The known presence of a child in a strike zone would most likely have prompted, at a minimum, further consideration of whether a more thorough assessment of the target was warranted.

Planners involved in the strike "had a genuine belief that there was an imminent threat to U.S. forces," the general said. He acknowledged that was "a mistake" but added that "it's not negligence."

General Said insisted that the strike has to be considered in the context of the moment, with American officials at a heightened state of alert after a suicide bombing at the Kabul airport three days earlier killed about 170 civilians and 13 U.S. troops.

The investigation made several recommendations for fixing the process through which strikes are ordered, including putting in new measures to cut down the risk of confirmation bias and reviewing the pre-strike procedures used to assess the presence of civilians.

Defense Secretary Lloyd J. Austin III ordered the review of the military's initial inquiry into the drone strike to determine, among other issues, who should be held accountable and "the degree to which strike authorities, procedures and processes need to be altered in the future."

Almost everything senior defense officials asserted in the hours, days and weeks after the drone strike turned out to be false. The explosives the military claimed were loaded in the trunk of a white sedan struck by the drone's Hellfire missile were probably water bottles. And a secondary explosion in the courtyard in the densely populated Kabul neighborhood where the attack took place was probably a propane or gas tank, officials said.

The driver of the white sedan that was struck by the American drone, Zemari Ahmadi, was employed by Nutrition and Education International, a California-based aid organization.

Gen. Kenneth F. McKenzie Jr., the head of Central Command, said in a news conference in September that the strike was carried out "in the profound belief" that the Islamic State was about to launch another attack on Hamid Karzai International Airport.

Since then, the Pentagon offered unspecified condolence payments to the family of the 10 civilians, including seven children, who were killed in the Aug. 29 drone strike.

	The Pentagon has also said it was working with the State Department to help surviving members of the family relocate to the United States. Congress has authorized the Pentagon to pay up to $3 million a year for payments to compensate for property damage, personal injury or deaths related to the actions of U.S. armed forces, as well as for "hero payments" to the family members of local allied forces, such as Afghan or Iraqi troops fighting Al Qaeda or ISIS. Condolence payments for deaths caused by the American military have varied widely in recent years. In fiscal 2019, for instance, the Pentagon offered 71 such payments — ranging from $131 to $35,000 — in Afghanistan and Iraq. "This investigation is deeply disappointing and inadequate because we're left with many of the same questions we started with," Dr. Steven Kwon, the president of Nutrition and Education International, said in an emailed statement. "I do not understand how the most powerful military in the world could follow Zemari, an aid worker, in a commonly used car for eight hours, and not figure out who he was, and why he was at a U.S. aid organization's headquarters." Critics of the strike pointed to the incongruity of acknowledging the mistake but not finding anyone responsible for any wrongdoing, a point that General Said touched on in his remarks. He said that he had sent the full report to senior military officials. "The fact that I've sent it to the chain of command, that doesn't mean the chain of command won't do anything," he said. "They can read this and say 'This is sub par performance.'" Hina Shamsi, director of the National Security Project at the American Civil Liberties Union, said in a statement that Nutrition and Educational International "and the surviving family members have repeatedly asked for meaningful transparency and accountability for the wrongful killing of their loved ones, but they did not receive it today. "The Inspector General's main findings of error, confirmation bias, and communication breakdowns are all too common with U.S. lethal strikes, and his recommendations do not remedy the tremendous harm here, or the likelihood that it will happen again." The Pentagon's initial acknowledgment of the mistaken strike came a week after a New York Times investigation of video evidence challenged assertions by the military that it had struck a vehicle carrying explosives meant for the airport.
Return to Top	

HEADLINE	**11/03 ISIS growing threat to Taliban govt.**
SOURCE	**https://www.nytimes.com/2021/11/03/world/asia/isis-afghanistan-taliban.html**
GIST	JALALABAD, Afghanistan — Aref Mohammad's war against the Islamic State ended earlier this fall when his unit of Taliban fighters was ambushed by the terrorist group in eastern Afghanistan. A bullet shattered his femur, leaving him disabled and barely able to walk, nevermind fight. But for the Taliban movement he served under, now the government of Afghanistan, the war against the Islamic State was just beginning. "If we knew where they were from, we would pursue them and destroy them," Mr. Mohammed, 19, said from his hospital bed in Jalalabad, the capital of Afghanistan's eastern Nangarhar Province where the Islamic State has maintained a presence since 2015. In the two months since the Taliban took control of the country, the Islamic State affiliate in Afghanistan — known as Islamic State Khorasan or ISIS-K — has stepped up attacks across the country, straining the new and untested government and raising alarm bells in the West about the potential resurgence of a group that could eventually pose an international threat.

The attacks have been aimed mostly at Taliban units like Mr. Mohammad's, and at Afghanistan's Shiite minorities. Suicide bombings in Kabul, the capital, and in important cities including Kunduz in the north and Kandahar in the Taliban's southern heartland have killed at least 90 people and wounding hundreds of others in the span of just several weeks. And on Tuesday, Islamic State fighters carried out a coordinated attack with gunmen and at least one suicide bomber on an important military hospital in the capital, killing at least 25 people.

This has placed the Taliban in a precarious position: After spending 20 years fighting as an insurgency, the group finds itself wrestling with providing security and delivering on its hallmark commitment of law and order. This has proved especially challenging for the Taliban as they try to defend themselves and civilians in crowded cities against almost daily attacks with an army that was trained for rural guerrilla warfare.

The surge in attacks has fueled growing unease among Western officials, with some predicting that the Islamic State — often considered a regional threat — could gain the capability to strike international targets in a matter of six to 12 months.

Colin Kahl, U.S. under secretary of defense for policy, told lawmakers last week that the Taliban's ability to pursue the group "is to be determined."

Mr. Kahl's sentiments underline the core concern of Western intelligence communities: There is little way to measure the Taliban's effectiveness against ISIS-K. There is no longer reliable access to intelligence as limited drone flights provide piecemeal information given the distance they have to fly just to get to Afghanistan, according to U.S. officials, and the established network of informants has collapsed.

The Taliban, who have refused to cooperate with the United States in countering the Islamic State, instead are fighting the war on their own terms, with tactics and strategies that look far more localized than a government campaign against a terrorist organization.

"The Taliban became accustomed to fighting as insurgents, relying on a range of asymmetric attacks to target Afghan and U.S. forces," said Colin P. Clarke, a counterterrorism analyst at the Soufan Group, a security consulting firm based in New York. "But it seems clear that the Taliban has not given much thought at all to how the equation changes as a counter insurgent, which is effectively the role they are playing now against the Islamic State."

But where the Taliban have changed their strategy to fight against the Islamic State — once working together with the Americans and the former government to contain the terrorist group in the east — is on the diplomatic stage.

As the Taliban seek international recognition, the group has used the resurgence of the terrorist group as a bargaining chip for more financial aid, according to Qatari officials, reminding other countries that a powerful Islamic State poses a threat to them as well.

Recognizing the potential threat along its shared border with Afghanistan, Pakistan is feeding some intelligence to the Taliban about the Islamic State, according to U.S. officials.

Dr. Basir, the head of the Taliban's intelligence arm in Jalalabad who only goes by one name, is one of the group's leaders adapting to fighting a war he was once on the other side of as a Taliban insurgent. He is now responsible for defending and securing a city of several hundred thousand people.

In the last several years, Jalalabad has been an easy target for the Islamic State, which has dispatched cells of fighters into the city from surrounding districts, carrying out assassinations and bombings at will.

But the group has taken advantage of the weeks during which the new government was coming together and has drastically widened its reach.

Between Sept. 18 and Oct. 28, the Islamic State has carried out at least 54 attacks in Afghanistan — including suicide bombings, assassinations and ambushes on security checkpoints, according to an analysis by ExTrac, a private firm that monitors militant violence in conflict zones. It amounts to one of the most active and deadly periods for the Islamic State in Afghanistan.

Most of those attacks have targeted Taliban security forces — a marked shift from the first seven months of the year, when the Islamic State primarily targeted civilians, including activists and journalists.

In countering the Islamic State, Dr. Basir said his men had adopted methods similar to the previous government, even relying on equipment used by the former intelligence service to intercept communications and radio traffic — tools gifted by the West over the last two decades in an effort to surveil the Taliban.

But he insisted that the Taliban have what the last government and Americans did not: the broad support of the local population, which has been a boon for the type of human intelligence capable of alerting authorities of attacks and fighter locations that had always been difficult to obtain in the past.

That level of trust and cooperation could wane, security analysts say, as there is increasing fear that the Taliban could use the ISIS-K threat as an excuse to carry out with impunity state-sponsored violence on certain segments of the population, such as members of the former government.

“There’s also a bit of a hubris and overconfidence because they think ISKP has such limited appeal in country — that, according to the Taliban, it is so beyond the pale that it will never have that widespread appeal so they think they can afford to ignore the threat,” said Ibraheem Bahiss, an International Crisis Group consultant and an independent research analyst.

In 2015, the Islamic State in Khorasan was officially established in Afghanistan’s east by former members of the Pakistani Taliban. The group’s ideology took hold partly because many villages there are inhabited by Salafi Muslims, the same branch of Sunni Islam as the Islamic State. A minority among the Taliban, who mostly follow the Hanafi school, Salafi fighters were eager to join the new terrorist group.

The draw of young fighters to the Islamic State is especially pronounced in Jalalabad, where Salafi mosques have sprung up in growing numbers in recent years, providing ample recruiting grounds for the terrorist group.

The Taliban have made a show of openness to the Salafists, accepting a pledge of allegiance from some Salafi clerics earlier this month. But there is still widespread unease within their community, especially in Jalalabad.

At one Salafi religious school in the city, the Taliban cracked down on the ideology by forcing the school’s founder to flee. They have allowed boys to continue their Quranic studies but have banned Salafist works from the curriculum.

For Faraidoon Momand, a former member of the Afghan government and a local power broker in Jalalabad, the worsening economic situation in the country is also driving the Islamic State’s recruitment.

“In every society if the economy is bad, people will do what they have to do to get by,” Mr. Momand said.

As dusk fell over Jalalabad on a recent day in October, a unit of Taliban fighters belonging to the intelligence agency rode through the streets in a modified Toyota pickup, a machine gun mounted in its bed, as the streets filled with commuters and evening shoppers.

The Talibs pulled up at key intersections and checkpoints, jumping out and assisting with the screening of cars and the ubiquitous yellow three-wheeled rickshaws that jostle and honk as they throng streets. They poked their heads in, shining flashlights inside, questioning passengers, and waved them on.

	"We have a court for every criminal," said Abdullah Ghorzang, a Taliban commander. "But there is no court for ISIS-K. They will be killed wherever they are arrested."
Return to Top	

Suspicious, Unusual

Top of page

HEADLINE	**11/03 Widow: 'where's the body' public autopsy?**
SOURCE	**https://www.king5.com/article/news/investigations/david-saunders-portland-autopsy-event-widow-wants-remains/281-5f7ad657-f3fb-443b-b022-d8039edecc67**
GIST	SEATTLE — "Where's the body?" That's the question a Louisiana widow asked after she learned her husband's body was publicly autopsied at an event in Portland, Oregon last month. Elsie Saunders, 92, of Baton Rouge, Louisiana learned of the event from a KING 5 investigation that went undercover at the cadaver class in a Marriott hotel ballroom on Oct. 17. Elsie thought her husband David Saunders' body had been donated to science, but it ended up being dissected in front of a live, paying audience. "Oh, I think is reprehensible," Elsie Saunders said during a phone call. "I think that this – they are using my husband's body. Like he's a performing bear or something." Event organizers sold tickets for up to $500 to the public to view in-person the autopsy and dissection of a human body. The event is part of the Oddities and Curiosities Expo, which travels across the country. A similar event scheduled for Halloween day in Seattle was canceled. David Saunders, 98, had registered to donate his body for medical research at Louisiana State University, but Elsie Saunders said the university wouldn't take it, because he died of COVID-19. David Saunders' body ended up at Las Vegas-based Med Ed Labs, which solicits body donations for medical research. The lab sold Saunders' body to the autopsy event, which was organized by DeathScience.org Founder Jeremy Ciliberto. Death Science recently sent an email to attendees of the Portland event, recommending they get tested for COVID-19, as they were unaware Saunders had died from the virus. "This was not something that we anticipated, as Med Ed Labs should have provided this information to us directly and we would not have proceeded further if this information would have been provided," the email reads. According to the CDC, risk of infection from a cadaver is low. DeathScience.org also claims in the email that the body was disinfected by the embalming process, but recommended everyone who was present at the live autopsy get tested for COVID-19 as a precaution. The company said it would not be working with Med Ed Labs on future events. Obteen Nassiri, a Med Ed Labs supervisor, said Ciliberto lied to his company about why his event wanted to purchase Saunders' body. Nassiri said the lab didn't know Saunders' body would be used for a paying audience. "We do not engage the donors' bodies in any kind of shows that it was involved with," Nassiri said. "We don't do anything like that."

	Ciliberto, who has no professional credentials, said it was up to Med Ed Labs to obtain consent for Saunders' body to be used in this way. However, Saunders' widow says that didn't happen – and Elsie Saunders wants to ensure it never happens again to another family. "You're totally helpless when you don't know what's happened," Saunders said. "And I didn't – I had no idea what happened until you communicated it with me." Church Funeral Services and Crematory, which handled the preparation of David Saunders' body before it was given to Med Ed Labs, told Elsie Saunders it would track down her husband's remains and cremate them for free. The funeral home then plans to return him to Elsie.
Return to Top	

HEADLINE	**11/03 Study: why world protesting so much**
SOURCE	**https://www.msn.com/en-us/news/world/why-is-the-world-protesting-so-much-a-new-study-claims-to-have-some-answers/ar-AAQiLfy**
GIST	**Are we in a historic age of protest?** A new study released Thursday that looked at demonstrations between 2006 and 2020 found that the number of protest movements around the world had more than tripled in less than 15 years. Every region saw an increase, the study found, with some of the largest protest movements ever recorded — including the farmers' protests that began in 2020 in India, the 2019 protests against President Jair Bolsonaro in Brazil and ongoing Black Lives Matter protests since 2013. Titled "World Protests: A Study of Key Protest Issues in the 21st Century," the study comes from a team of researchers with German think tank Friedrich-Ebert-Stiftung (FES) and the Initiative for Policy Dialogue, a nonprofit organization based at Columbia University and adds to a growing body of literature about our era of increasing protests. Looking closely at more than 900 protest movements or episodes across 101 countries and territories, the authors came to the conclusion that we are living through a period of history like the years around 1848, 1917 or 1968 "when large numbers of people rebelled against the way things were, demanding change." But why? Here, the authors highlight one particular problem: democratic failure. Their research found that a majority of the protest events they recorded — 54 percent — were prompted by a perceived failure of political systems or representation. Roughly 28 percent included demands for what the authors described as "real democracy," the most of any demand found by the researchers. Other themes included inequality, corruption and the lack of action over climate change. But the study's authors say policymakers do not respond adequately. "Too many leaders in government and business are not listening. The vast majority of protests around the world advance reasonable demands already agreed upon by most governments. People protest for good jobs, a clean planet for future generations, and a meaningful say in the decisions that affect their quality of life," said Sara Burke, senior expert on global economic policy at the FES and an author on the study. **Protests mean different things to different people.** The study was released the same week that The Washington Post released a massive, three-part investigation into the Jan. 6 insurrection that began, in part, as a protest about some participants' concerns, stoked by conspiracy theories, about democratic representation. There will also be significant climate change protests later this week — but some European leaders are concerned that the costs of shifting away from fossil fuels could spark a backlash like the "yellow vest" protest movement in France. In the United States alone, recent years have seen huge protests from Occupy Wall Street and Black Lives Matter to the Tea Party and Stop the Steal campaigns. But tracking the scale of global protests is a mammoth task. Other projects, such as the Google-backed Global Database of Events, Language, and Tone, have scraped news articles for data about protests. Burke, along with co-authors Isabel Ortiz, Mohamed Berrada and Hernán Saenz Cortés, instead took a more time-consuming method. Researchers

worked across news mediums in seven languages to identify protests and protest movements — finding articles "by hand" as Burke put it in response to questions from Today's WorldView.

The collection alone represented more than a thousand hours of work before any analysis had even started. But the trends were clear. In 2006, just 73 protest movements were recorded by the study. In 2020, there were 251 — higher even then after the 2008 financial crisis or the Arab Spring revolts of 2011. Europe and Central Asia had seen the largest increase in the number of protest movements and there were more protests in high-income countries than in countries in other income brackets, but a rise in protests was found across all regions and income levels.

(The authors kept records of protest movements across different years, marking them as separate "protest events" when they spanned more than one year for a grand total of 2,809. This does not mean that only 2,809 individual protests occurred; other studies have put the number of Black Lives Matter protests at nearly 12,000 in 2020 alone.)

Other than issues with democracy and political representation, the report identifies rising inequality as another broad theme of protests around the world, contributing to nearly 53 percent of the protests studied. Individual issues raised by protesters included corruption, labor conditions, and reform of public services followed "real democracy" as the most widely cited.

There was also a significant increase in demands for racial or ethnic justice, such as with the Black Lives Matter protests, but there was a small — but growing — number of protests focused on denying the rights of others during the period, with the authors pointing toward Germany's far-right "Pegida" movement, anti-Chinese movements in Kyrgyzstan and the "yellow vest" movement among them.

The study's authors acknowledge that their work is inherently political. "There are no neutral numbers in protests," Burke said, admitting that the vagueness of some numbers, such as crowd size estimates, left items open for interpretation. An Internet-based study is also limited by what is reported. "We can only study what we can see and what we can see is increasingly impacted by where and who we are," Burke added.

Asked what defines "real democracy," Burke admitted it was somewhat subjective: "One person's democracy is another person's autocracy." But the study tried to take protesters at their word. In the case of Jan. 6, 2021, in Washington D.C. (which was not included in the study as it was outside of its time frame), Burke said that, too, would have been classified as a demonstration for "real democracy" but also a protest designed to deny rights, among other designations.

Most protests aren't violent like the Capitol insurrection, the study found, but there has been a slow but steady increase in violence between 2006 and 2020, with just over one-fifth of recorded protests involving some kind of crowd violence, vandalism or looting. In almost half of the protests studied, there were reports of arrests; a little over a quarter saw reports of some form of violence from the police.

Perhaps the key argument from the study is that as protests increase, leaders should take them more seriously. Roughly 42 percent of protests in the study were judged as successful, though that varied significantly by region and the type of protests and included partial successes — a higher figure than some other studies. If our era of protests continues, that suggests many more protesters are going to get at least some of what they want.

"Protests around the world have been getting a dubious reputation lately," said Michael Bröning, director of the FES New York office. "We need to understand that protests are not a verboten behavior but a core tenet of democracy. What we need is nothing short of a global rehabilitation of protest."

Return to Top

HEADLINE	**11/03 Another Oregon county looks to join Idaho**
SOURCE	**https://www.seattletimes.com/seattle-news/politics/another-oregon-county-looks-to-join-idaho/**

GIST	BURNS, Ore. (AP) — Another rural, conservative county in Oregon has expressed interest in becoming part of Idaho. The OregonianLive reports that voters in Harney County on Tuesday approved a ballot measure which requires local officials to hold meetings about moving the county into Idaho. The measure passed with more than 63% of the vote. The unofficial results were: 1,567 for and 917 against. Harney became the eighth of Oregon's 36 counties to vote for considering adjusting Oregon's border to put much of rural eastern and southern Oregon in Idaho. "Rural Oregon is declaring as loudly as it can that it does not consent to being misgoverned by Oregon's leadership and chooses to be governed as part of a state that understands rural Oregon's values and way of making a living," said Mike McCarter, who heads Move Oregon's Border for a Greater Idaho, which is behind the initiatives. These ballot initiatives are non-binding; the point of them, McCarter says, is to force Idaho's and Oregon's legislatures to take up the issue, which is highly unlikely. If Idaho and Oregon were to negotiate a border adjustment, the U.S. Congress would have to sign off on it. The other counties that have voted for a Move Oregon's Border-backed initiative in the last two years: Baker, Grant, Jefferson, Lake, Malheur, Sherman and Union. Two small counties have voted against the border-moving idea. Douglas and Klamath counties likely will be next to vote.
Return to Top	

HEADLINE	**11/03 Report: cannabis state's 4th valuable crop**
SOURCE	**https://www.seattletimes.com/business/cannabis-is-washingtons-4th-most-valuable-crop-industry-report-says/**
GIST	Apples may be Washington's biggest cash crop, but legal cannabis is gaining ground. Growers in Washington generated wholesale revenues of $653 million on 561,000 pounds of legal weed in 2020, according to a new estimate by Leafly, a Seattle-based cannabis marketplace and information site. That makes cannabis Washington's fourth most valuable legal crop, behind only apples ($2.1 billion), wheat ($949 million) and potatoes ($753 million), but ahead of cherries ($562 million) and hay ($501 million), according to figures from the U.S. Department of Agriculture. It's also enough to rank Washington as the fourth biggest producer of legal cannabis, by wholesale revenues, among the 11 states with legal recreational sales, which last year totaled $6.2 billion in wholesale revenues, according to Leafly. California leads the U.S., with $1.7 billion, followed by Colorado ($1 billion) and Michigan ($736 million). Washington and Colorado were the first states to legalize sales of recreational cannabis, in November 2012. Washington had its first commercial crop in 2014. The state currently has 1,070 licensed producers or producer/processors, according to the state Liquor and Cannabis Board. Leafly released the wholesale estimates for Washington and other states in part because legal cannabis still lacks the recognition that other agricultural crops get as a source of economic value. "Cannabis is now Washington's 4th most valuable agricultural crop," said Leafly editor Bruce Barcott. "But Washington's ag community and state ag agencies still refuse to recognize cannabis farmers as farmers."

	Indeed, because cannabis isn't federally legal, it's not in the USDA data that Washington and other states use in their own yearly rankings of farm output, state and federal agriculture officials said. Lack of federal status also means Washington's cannabis farmers don't get the same benefits and protections that most other farmers do. They are excluded from protections under Washington's Right to Farm Act, which shields farmers from nuisance lawsuits by neighbors. They also can't get the state property and estate tax reductions that farmers get for croplands, and aren't entitled to federal farm assistance programs, state officials say. States typically publish data on retail sales and taxes, but there's little available publicly on revenues that cannabis brings to farmers, Barcott said. To calculate Washington's wholesale figure, Leafly estimated that every dollar in retail sales generated 47 cents in wholesale sales, Barcott said. In 2020, Washington reported around $1.4billion in retail cannabis sales, according to calculations from LCB data. Leafly only estimated wholesale revenues for 2020. But applying Leafly's percentage to earlier years in Washington suggests that wholesale cannabis revenues have grown from around $68 million in 2015 to around $454.5 million in 2018 and $653 million in 2020. Washington's illegal cannabis industry, meanwhile, has shrunk considerably under pressure from legal weed, which was cheaper than its illegal counterpart soon after the state industry launched, LCB officials said. The agency has no firm estimates for how much illegal weed is still grown in Washington, but acknowledges that some remains. "Today, we mostly see only large-scale [illegal] operations prepping to divert out of state to states that haven't legalized," said LCB spokesperson Brian Smith. Even though state and federal agencies don't rank cannabis as a farm commodity, Leafly's effort earned a nod from Christopher Mertz, USDA's Northwest regional director, who called it "a fair attempt at trying to see where that industry sits with other U.S. crops."
Return to Top	

HEADLINE	**11/03 Arctic warms: forecasting shifting sea ice**
SOURCE	**https://www.wired.com/story/as-the-arctic-warms-ai-forecasts-scope-out-shifting-sea-ice/**
GIST	**FOR GENERATIONS, THE** inhabitants of the Arctic have counted on seasonal sea ice, which grows and retreats during the year. Polar bears and marine mammals rely on it as a hunting spot and a place to rest; Indigenous people fish from openings in the ice known as polynyas, and use well-known routes across the ice to travel from place to place. But the Arctic air and water has warmed three times faster than the rest of the planet since 1971, according to a May 2021 report by the Arctic Council, and this warming is causing the ice to expand and contract in unpredictable ways. Some scientists and research firms are now deploying tools powered by artificial intelligence to provide more accurate and timely forecasts of what parts of the Arctic Ocean will be covered with ice, and when. AI algorithms complement existing models that use physics to understand what's happening at the ocean's surface, a dynamic zone where cold underwater currents meet harsh winds to create floating rafts of ice. This information is becoming increasingly valuable for tribal members in the Arctic, commercial fishers in places like Alaska, and global shipping companies interested in taking shortcuts through open patches of water. Leslie Canavera, CEO of Polarctic, a Lorton, Virginia–based scientific consulting firm that has developed AI-based forecast models, says the uncertain pace of climate change means that existing models of sea ice are becoming less accurate. That's because they are based on environmental processes that are quickly shifting.

“We don't have a great understanding of climate change and what's happening in the [Arctic] system,” says Canavera, who is a Yup’ik tribal member and grew up in Alaska. “We have statistical modeling, but then you're looking at more of the averages. Then you have artificial intelligence, where it's able to see the trends in the system and learn.”

Existing physics-based models capture hundreds of years of scientific records about ice conditions, current meteorological conditions, the speed and location of the polar jet stream, the amount of cloud cover, and ocean temperature. The models use that data to estimate future ice coverage. But it takes large amounts of computing power to crunch the numbers, and several hours or days to produce a forecast using conventional programs.

While AI also requires complex data and a lot of initial computing power, once an algorithm is trained on the right amount and kind of data, it can detect patterns in climate conditions more quickly than physics-based models, according to Thomas Anderson, a data scientist at the British Antarctic Survey who developed an AI ice forecast called IceNet. “AI methods can just run thousands of times faster, as we found in our model, IceNet,” Anderson says. “And they also learn automatically. AI is not smarter. It's not replacing physics-based models. I think the future is leveraging both sources of information.”

Anderson and his colleagues published their new sea ice forecast model in August in the journal *Nature Communications*. IceNet uses a form of AI called deep learning (also used to automate detection of credit card fraud, operate self-driving cars, and run personal digital assistants) to train itself to provide a six-month forecast in each 25-kilometer square grid across the region, based on simulations of the Arctic climate between the years 1850 to 2100 and actual observational data recorded from 1979 to 2011. Once the model was trained and given current meteorological and ocean conditions, IceNet beat a leading physics-based model in making seasonal forecasts about the presence or absence of sea ice in each grid square, particularly for the summer season, when the ice goes through an annual retreat, according to the *Nature* study.

A separate team of scientists at the Johns Hopkins University Applied Physics Laboratory has developed a forecast model that uses a form of AI called convolutional neural networks to examine satellite images of the ocean surface and make predictions of how quickly ice will form in the coming week. Neural networks are able to sort digital pixels more quickly than humans, and are used in facial recognition algorithms, for example. The JHUAPL model uses digital satellite images and combines them with meteorological data that is collected on the ground at the same time , according to Christine Piatko, a senior staff scientist at the laboratory and principal investigator on the project.

Right now, forecasters at the US National Ice Center in Colorado compile weekly Arctic ice forecasts by hand, analyzing images taken by orbiting satellites and comparing them with historic data. But that method might not be good enough now that the Arctic Sea is rapidly losing its ice cover. In fact, it may be completely ice-free in the summer months by 2050, according to estimates by a group of 21 research institutions published in 2020.

The opening of the Arctic Sea means more ship traffic, and more ships means better forecasts are needed, Piatko says. Until now, physics-based models and manual estimates of ice coverage have been adequate. Forecasters “only had to make forecasts for a few ships or for special missions,” Piatko says. “But as there's increased activity, you can imagine different scenarios where they might need information in a more timely manner. We are trying to anticipate that need.”

Polarctic’s Canavera is collaborating with Canadian officials to develop ice forecasts for residents of the territory of Nunavut, and develop better understanding of critical food resource areas that are changing thanks to climate change. A separate project called SmartIce uses data from small battery-powered sensors embedded in the sea ice that record both temperature and ice thickness, and that information can be used to aid navigation and keep Indigenous people safe.

Her firm is also developing localized sea ice forecasts for Alaskan commercial harvesters who want to

	fish at the edge of the ice, which is a productive area for cod and crabs. “You need a strong forecast of where the ice edge is going to be and how it's going to change. Because if the ice comes in too fast, or the forecast is wrong, then the fishermen can lose their fishing gear—it becomes ghost plastic in the ocean, and they're out of profits,” Canavera says. “We’re hoping to solve that problem and develop a solution.” Forecasting sea ice is just one application of artificial intelligence as scientists try to understand the changing climate. AI algorithms can also be deployed to forecast electric power supply, demand, and carbon dioxide emissions; automate detection of methane leaks; and even predict improvements in energy efficiency of office buildings and homes, according to a 2019 paper by a group of 22 renowned computer scientists presented at the world’s leading AI conference, known as NeurIPS. Anderson and his Icenet colleagues are aiming to boost the IceNet model’s accuracy to forecast ice conditions at greater resolution down to grids that are only several hundred meters across rather than 25 kilometers. But still, he says that AI models are no substitute for the on-the-ground knowledge of Arctic coastal residents. “Nothing beats being on the shoreline and saying, ‘You know, I cannot go out onto the sea ice today, because the sea ice is too thin or there's no platform,’” he says. “But what these predictions can do is give people a general sense of, okay, what is the trajectory of the ice in the surrounding area? That's filling a really big and important gap, where advances in AI forecasting could make a huge difference.”
Return to Top	

HEADLINE	**11/04 NKorea can make more uranium for bombs**
SOURCE	**https://www.wsj.com/articles/north-korea-can-make-more-uranium-for-nuclear-bombs-than-previously-thought-11636006162?mod=hp_listb_pos1**
GIST	SEOUL—North Korea has the capacity to make more base ingredients for nuclear bombs than previously believed, according to new research, suggesting the Kim Jong Un regime possesses the potential to accelerate the earliest stages of production. The nation’s output of uranium—a fissile material for nuclear weapons when enriched—is just a fraction of what could be produced, according to new research from Stanford University’s Center for International Security and Cooperation. The assertion is based on satellite-imagery analysis of the equipment and facility size of the Kim regime’s only confirmed operational uranium mining complex in Pyongsan county, about 30 miles north of the Korean Demilitarized Zone. That milling capacity assessment was contrasted with North Korea’s estimated production, based on the levels of waste deposited near the mill. Furthermore, researchers tracked deforestation levels to study mining activity from 2017 to 2020, using an algorithm to analyze satellite imagery and detect land-use changes. The gap between potential and actual production may indicate that the Kim regime is satisfied with its current proliferation levels, doesn’t have enough ore to mine or that potential bottlenecks exist at later stages of weapons-grade fissile development, said Sulgiye Park, the report’s lead author who is a nuclear-security research fellow at Stanford. “It’s using 1/10th or 1/20th of the capacity it has,” Ms. Park said. “The big question is why.” Though denuclearization talks have stalled in recent years, North Korea hasn’t halted its weapons development. It test-launched a range of shorter-range missiles in recent weeks and is pushing forward on fissile-material production. North Korean leader Mr. Kim has vowed recently to keep pursuing weapons advances to face the threat from the U.S. and South Korea—accusing both countries of having adopted hostile policies.

Uranium can be found around the world and typically gets used as the fuel for nuclear power plants. But when enriched to a weapons grade of roughly 90% purity, uranium can be used in atomic weapons to set off a chain reaction that creates a nuclear explosion.

At Pyongsan, ore gets crushed, sorted and processed, before the uranium gets extracted, purified and dried into yellowcake that gets transported elsewhere for further enrichment, according to the Stanford report. Uranium can also be used in reactors to make plutonium.

Decades-old estimates of North Korea's annual uranium ore output were put at roughly 30,000 metric tons, the report said. But the capacity could be as much as 360,000 metric tons, according to the Stanford analysis, which factored in Pyongsan's milling infrastructure, size and equipment. The estimate assumes optimal operations for 300 days a year.

To assess Pyongsan's ore quality, Ms. Park, a trained geologist, collected samples from South Korea, as well as rock analysis of other places with similar geological formations.

The findings suggest the Kim regime could process enough yellowcake for up to 340 kilograms of highly enriched uranium a year—enough for more than 20 nuclear bombs annually. In a 2020 assessment, the U.S. Army said North Korea has the ability to manufacture six new bombs a year.

The Stanford report cited other research that estimates North Korea can enrich the equivalent of roughly six to 10 nuclear bombs a year. That means even if Pyongsan churned out much higher levels of yellowcake, expanding fissile-material production would likely face constraints at the North's Yongbyon facility, where such enrichment work is believed to be done.

"Pyongsan is your first stop for North Korea's nuclear program because it has the one identifiable mine that we know of," said Dave Schmerler, a senior research associate at the James Martin Center for Nonproliferation Studies, who has done satellite-imagery analysis of Pyongsan though was uninvolved in the Stanford report.

Dismantling the Pyongsan uranium concentrate plant should be an essential component of any denuclearization talks between the U.S. and North Korea, according to the Center for Strategic and International Studies, a Washington-based think tank, which has published satellite-imagery reports about the mining facilities.

North Korea hasn't allowed outside nuclear inspectors into the country for more than a decade. Pyongsan was one of several key sites, including Yongbyon, that International Atomic Energy Agency officials visited in the early 1990s.

The Stanford estimates had limitations by relying on satellite imagery, Ms. Park said. Collecting samples from Pyongsan itself would allow her to study rock cross sections to better determine ore quality. Spot checks could provide greater confidence that changes to Pyongsan's topography arose from mining and not something else.

The U.N.'s atomic agency, in a report submitted in August, said North Korea had appeared to have resumed operation of its plutonium-producing reactor at its Yongbyon facility. The reactor had been inactive since December 2018 until the beginning of July 2021. A nearby laboratory that separates plutonium from spent fuel had also shown signs of being operational around that time.

The mining activities continued at Pyongsan, even last year when North Korea became one of the first countries in the world to seal off its borders as neighboring China began reporting widespread Covid-19 infections.

The Stanford analysis, in contrast with prior reports that focused more on bursts of activity than geological science, tracked deforestation and land-use developments by using algorithms developed by Orbital Insight Inc., whose software can automatically detect such changes. Normally such analysis can take hours

	to fully characterize what is in a single image, though the algorithms reduced that process to just seconds, said Olivia Koski, an Orbital Insight employee involved in the Stanford research. In future research using Orbital's imagery detection tools, an analysis of railcar activity from Pyongsan to North Korea's Yongbyon facility could offer even more precise measurements on how much yellowcake the country is producing, Ms. Park said. Railway and milling activity was detected as recently as late last month at Pyongsan, she added. "The activity at this site never really slowed down during Covid," she said.
Return to Top	

HEADLINE	**11/03 Report: 18 billionaires got stimulus checks**
SOURCE	**https://www.cbsnews.com/news/stimulus-check-billionaires-wealthy/**
GIST	At least 18 billionaires — and hundreds of other ultra-wealthy individuals — received federal stimulus checks even though the payments were aimed at helping poor and middle-income households weather the pandemic's economic crisis, according to a new report from ProPublica. About 270 wealthy people received payments in the first round of stimulus checks directed by lawmakers in 2020, despite having a total of $5.7 billion in income, according to the report, which cited a trove of IRS data on thousands of the nation's wealthiest individuals ProPublica said it had obtained. These rich taxpayers received stimulus checks after tapping complex tax deductions to reduce their net incomes to less than zero, qualifying them for the checks, the report noted. Under the law, the full payments of $1,200 per single taxpayer and $2,400 for married couples were only available to single people earning less than $75,000 or couples with incomes below $150,000. Included among the billionaires who received stimulus checks are philanthropist George Soros, worth $7.5 billion, according to the Bloomberg Billionaires Index, and financier Ira Rennert, worth $3.7 billion, the report noted. Soros' representative said he returned the check, while Rennert didn't respond to questions, ProPublica said. To be sure, the bulk of stimulus payments were directed to households that legitimately qualified for the checks, but the fact that billionaires received the aid underscores how differently the U.S. tax system works for the ultra-rich. The 270 wealthy people who got the checks most certainly didn't request the payments — the IRS automatically directed the aid to anyone it determined qualified by income. It may seem mind-boggling that a billionaire could qualify for a $1,200 check from a stimulus program with an income threshold of $75,000 per single taxpayer. But because these billionaires tapped write-offs, deductions and other loopholes to minimize their incomes, they appeared to the IRS to have net incomes of less than zero, making them eligible for the payments. "This disgrace is why we need real tax reform," the Institute on Taxation and Economic Policy, a left-leaning think tank, said on Twitter about the findings. The ProPublica report comes as some Democratic lawmakers are pushing for a tax on billionaires, arguing that the nation's wealthiest citizens should pay more as a matter of fairness. During the pandemic, the collective net worth of America's roughly 700 billionaires surged by $2 trillion, thanks to a rise in stock prices and the values of other assets, according to Americans for Tax Fairness, a left-leaning group. The billionaires tax would place a new levy on asset gains, whether a billionaire has sold the asset or not. Under current law, a gain is only taxed if it is "realized" when its owner sells the asset and books the profit. Unrealized gains — stocks or other investments that rise in value and that the investor holds onto and leverage — aren't currently taxed.

	But the finding that at least 18 American billionaires received stimulus checks earmarked for middle-income families reveals how differently the current tax system works for the wealthy. Most people pay taxes on earned income, such as their salaries or earnings from gig work, which is reported to the IRS on W2 or 1099 statements. The ultra-wealthy, however, have a host of accounting tricks and deductions they can use to reduce their reported income, such as by using business losses to offset income. Those valuable deductions can effectively minimize their tax liabilities — and, apparently, help them qualify for stimulus checks.
Return to Top	

HEADLINE	**11/03 Globe bounces back to 2019 carbon levels**
SOURCE	**https://abcnews.go.com/Technology/wireStory/globe-bounces-back-2019-carbon-pollution-levels-80961378**
GIST	GLASGOW, Scotland -- The dramatic drop in carbon dioxide emissions from the pandemic lockdown has pretty much disappeared in a puff of coal-fired smoke, much of it from China, a new scientific study found. A group of scientists who track heat-trapping gases that cause climate change said the first nine months of this year put emissions a tad under 2019 levels. They estimate that in 2021 the world will have spewed 36.4 billion metric tons of carbon dioxide, compared to 36.7 billion metric tons two years ago. At the height of the pandemic last year, emissions were down to 34.8 billion metric tons, so this year's jump is 4.9%, according to updated calculations by Global Carbon Project. While most countries went back to pre-pandemic trends, China's pollution increase was mostly responsible for worldwide figures bouncing back to 2019 levels rather then dropping significantly below them, said study co-author Corinne LeQuere, a climate scientist at the University of East Anglia in the United Kingdom. With 2020's dramatically clean air in cities from India to Italy, some people may have hoped the world was on the right track in reducing carbon pollution, but scientists said that wasn't the case. "It's not the pandemic that will make us turn the corner," LeQuere said in an interview at the climate talks in Glasgow, where she and colleagues are presenting their results. "It's the decisions that are being taken this week and next week. That's what's going to make us turn the corner. The pandemic is not changing the nature of our economy." If the world is going to limit global warming to 1.5 degrees Celsius (2.7 degrees Fahrenheit) since pre-industrial times, it has only 11 years left at current emission levels before it is too late, the paper said. The world has warmed 1.1 degrees Celsius (2 degrees Fahrenheit) since the late 1800s. "What the carbon emissions numbers show is that emissions (correcting for the drop and recovery from COVID19) have basically flattened now. That's the good news," said Pennsylvania State University climate scientist Michael Mann, who wasn't part of the report. "The bad news is that's not enough. We need to start bringing (emissions) down." Emissions in China were 7% higher in 2021 when compared to 2019, the study said. By comparison, India's emissions were only 3% higher. In contrast, the United States, the European Union and the rest of the world polluted less this year than in 2019. LeQuere said China's jump was mostly from burning coal and natural gas and was part of a massive economic stimulus to recover from the lockdown. In addition, she said, China's lockdown ended far earlier than the rest of the world, so the country had longer to recover economically and pump more carbon into the air.

	The “green recovery” that many nations have talked about in their stimulus packages take longer to show up in emission reductions because rebounding economies first use the energy mix they already had, LeQuere said. The figures are based on data from governments on power use, travel, industrial output and other factors. Emissions this year averaged 115 metric tons of carbon dioxide going into the air every second. Breakthrough Institute climate director Zeke Hausfather, who wasn’t part of the study, predicts that “there is a good chance that 2022 will set a new record for global CO2 emissions from fossil fuels.”
Return to Top	

Crime, Criminals

Top of page

HEADLINE	**11/03 Federal Way police homicide investigation**
SOURCE	https://www.kiro7.com/news/local/body-teenager-found-park-police-investigating-homicide/6FJIVKPE6ZGHLG5VKVQKNPFDOE/
GIST	FEDERAL WAY, Wash. — Federal Way police have opened a homicide investigation after finding a body in a park near the 37200 block of 20 Avenue South. “The type of neighborhood you look to move into,” said David Lopez. He and his wife Ashlee moved into the neighborhood nearly a year ago with their two kids. “It’s the type of neighborhood where you look to raise your family,” he says. What they thought would be a quiet community changed overnight, when they say they were awoken around 3:30 a.m. by a loud noise that sounded like a gunshot. “Immediately after that I heard three more,” said Ashlee Lopez. After checking with neighbors and knowing the police had already been called, the couple went back to bed. It wasn’t until the next morning when Ashlee Lopez was taking her daughter to school, when she made a horrific discovery. “We pulled out of this driveway and I noticed something on the grass in the park,” said Ashlee Lopez. “I got out of the car and walked over until I was just a couple of feet away, and saw that there was some blood on the gentleman’s face.” Federal Way police say the person shot and killed was a 13-year-old. Officers didn’t say if the child was shot, but the Lopez family believes its connected to the gunfire they heard overnight. “We have a 16-year-old and a 12-year-old, so to see somebody the same age as our son lying on the ground like that in a violent way is tragic,” says David Lopez. Police have not yet released any information on the shooter.
Return to Top	

HEADLINE	**11/03 Lakewood police investigate explosion**
SOURCE	https://www.q13fox.com/news/explosion-shakes-lacey-police-investigating
GIST	LACEY, Wash. - Lacey Police are investigating what they are calling a "homemade explosive device" set off in the woods Wednesday afternoon. Police say the incident happened around 1 p.m. in Lacey off of Yelm Highway Southeast and College street, near the shopping center.

	Lacey Police say they found a partially exploded device in a wooded area. Surveillance footage from a nearby home caught the explosion. "All of a sudden I heard a big boom and we were like what just happened," said Stephanie Rozier. Rozier's camera caught the blast. She tells FOX 13 News she felt the house shake when the explosion went off. "I looked out the back window and saw smoke everywhere. So, we looked and saw that it was right there, not even 30 feet from the house," she said. Rozier says what is most unsettling is these explosions keep happening. "We don't know who it is. And since it keeps getting bigger are they eventually going to make one and it's going to blow up the house, we don't know," she said. She says she hopes the attention on this most recent explosion will deter any future incidents. No one was injured in the explosion, authorities say.
Return to Top	

HEADLINE	**11/03 Tacoma police: man found shot in vehicle**
SOURCE	**https://www.q13fox.com/news/tacoma-police-investigating-after-man-found-shot-in-vehicle**
GIST	**TACOMA, Wash.** - Tacoma Police are investigating after a man was found shot inside a vehicle. Officers responded to the 3900 block of Mason Loop Road just before 8:30 p.m. on Nov. 3 for reports of a shooting. When they arrived, they found a 32-year-old man shot inside a vehicle. The victim was taken to the hospital with serious injuries. The investigation is ongoing. It's unclear if the victim was targeted. Police have not released any suspect information.
Return to Top	

HEADLINE	**11/04 Philadelphia bans pretextual traffic stops**
SOURCE	**https://apnews.com/article/philadelphia-gun-politics-jim-kenney-3303e90208819de3394773c60c2815aa**
GIST	PHILADELPHIA (AP) — The mayor ordered police Wednesday to stop pulling over drivers for low-level offenses that critics say lead to disproportionate stops of minority drivers, making Philadelphia the largest city government in the U.S. to ban what are sometimes called pretextual stops. The executive order from Mayor Jim Kenney puts a bill passed last month by the City Council — called the Driving Equality Bill — into effect. It bans officers from pulling over vehicles solely for a handful of traffic offenses deemed “secondary violations,” such as improperly displayed registration or inspection stickers, and single broken taillights. Advocates for law enforcement say such stops can uncover illegal drugs and weapons, noting that the U.S. Supreme Court ruled in 1996 that they were acceptable. But critics say the practice has led to Black and Latino motorists being unfairly stopped and searched at high rates and sometimes being detained for small infractions.

	It has also led to a handful of high-profile deaths. Sandra Bland in Texas, Walter Scott in South Carolina and Duante Wright in Minnesota were all initially pulled over for pretextual stops. At least two prosecutor's offices in Minnesota have said they will no longer prosecutor motorists charged with other crimes resulting from pretextual stops. Municipalities smaller than Philadelphia, the nation's sixth-most populous city, have issued similar bans, and the state of Virginia banned stops solely for infractions like smelling marijuana, overly tinted windows or objects hanging from the rearview mirror. The Defender Association of Philadelphia projected that the enforcement change could mean as many as 300,000 fewer police encounters a year. The order also put into effect a second bill passed by the City Council requiring Philadelphia to collect and publish data on traffic stops, including the reason for the initial stop, the demographics of the driver and passengers, and the locations of those stops. In 2011, the city settled a policing discrimination lawsuit that alleged Philadelphia officers illegally targeted Black residents for pedestrian searches. Reform advocates have argued in recent years that because those pedestrian stops have been closely monitored, officers turned to pretextual traffic stops to conduct the same barred searches on Black drivers instead.
Return to Top	

HEADLINE	**11/04 Venezuela faces landmark ICC investigation**
SOURCE	**https://www.theguardian.com/world/2021/nov/04/venezuela-faces-landmark-icc-investigation-over-alleged-crimes-against-humanity**
GIST	The international criminal court (ICC) is opening a formal investigation into allegations of torture and extrajudicial killings committed by Venezuelan security forces under President Nicolás Maduro's rule, the first time a country in Latin America is facing scrutiny for possible crimes against humanity from the court. The opening of the probe was announced Wednesday by ICC chief prosecutor Karim Khan at the end of a three-day trip to Caracas. Standing alongside Maduro, Khan said he was aware of the political "fault lines" and "geopolitical divisions" that exist in Venezuela. But he said his job was to uphold the principles of legality and the rule of law, not settle scores. "I ask everybody now, as we move forward to this new stage, to give my office the space to do its work," he said. "I will take a dim view of any efforts to politicise the independent work of my office." While Khan didn't outline the scope of the ICC's investigation, it follows a lengthy preliminary probe started in February 2018 — later backed by Canada and five Latin American governments opposed to Maduro — that focused on allegations of excessive force, arbitrary detention and torture by security forces during a crackdown on antigovernment protests in 2017. Human rights groups and the US-backed opposition immediately celebrated the decision. Since its creation two decades ago, the ICC has mostly focused on atrocities committed in Africa. "This is a turning point," said Jose Miguel Vivanco, the Americas director for Human Rights Watch. "Not only does it provide hope to the many victims of Maduro's government but it also is a reality check that Maduro himself could be held accountable for crimes committed by his security forces and others with total impunity in the name of the Bolivarian revolution." It could be years before any criminal charges are presented as part of the ICC's investigation.

	Maduro said he disagreed with Khan's criteria in choosing to open the probe. But he expressed optimism that a three-page "letter of understanding" he signed with the prosecutor that would allow Venezuelan authorities to carry out their own proceedings in search of justice, something allowed under the Rome statute that created the ICC. "I guarantee that in this new phase we will leave the noise to the side and get down to work so that, together, the truth can be found," said Maduro. Maduro's government last year also asked the ICC to investigate the US — which is not among the ICC's 123 member states — for its policy of economic sanctions focused on removing Maduro. Venezuela considers the US sanctions tantamount to "unlawful coercive measures" that have spelled poverty for millions of Venezuelans. Khan's predecessor, Fatou Bensouda, had indicated there was a reasonable basis to conclude that crimes against humanity had been committed in Venezuela, echoing the findings of the UN's own human rights council last year. But she left the decision to open any probe to her successor Khan, a British lawyer who took the reins of the ICC earlier this year.
Return to Top	

HEADLINE	**11/03 OECD: counterfeit products flood internet**
SOURCE	**https://www.cbsnews.com/news/counterfeit-products-abound-internet-ahead-of-holidays/**
GIST	The COVID-19 pandemic has driven even more consumers to do their shopping online, particularly around the holidays, in order to avoid in-store contact. But making purchases over the internet can be risky, too. Take Aaron Muderick, founder of Crazy Aarons magnetic putty, who on Tuesday told a Senate committee that listings for products that imitate his made by overseas manufacturers have cropped up online. He testified that hundreds of third-party sellers are selling counterfeit — and unsafe — versions of his putty. "These bad actors often sell unsafe goods which do not meet the stringent federal safety standards required of legitimate producers," Muderick said. For example, a magnet used in Crazy Aarons' product is large enough that it doesn't present a choking hazard. But magnets used in other online products fit easily inside a tube used to measure unsafe product components, CBS News correspondent Elise Preston reported. The Organisation for Economic Co-operation and Development's latest report on counterfeit and pirated goods shows that such products have proliferated with the rise of ecommerce, and now make up more than 3% of all global trade. The sale of these counterfeit goods can hurt legitimate companies' sales as well as consumers. As a result, Congress is considering legislation, called the Inform Act, that is designed to curtail the sale of counterfeit goods online and requires marketplaces to verify sellers' identities Amazon, Etsy and Ebay, all members of the Internet Association, a lobbying group, each endorse the House version of the bill.
Return to Top	

HEADLINE	**11/03 Judge: Arbery trial jury makeup stands**
SOURCE	**https://www.cbsnews.com/news/ahmaud-arbery-trial-jurors/**
GIST	Brunswick, Georgia — A judge ruled Wednesday that he'll seat one Black juror and 11 whites to decide the trial of the men who chased and killed Ahmaud Arbery, despite prosecutors' objections that several Black potential jurors were cut because of their race.

Superior Court Judge Timothy Walmsley acknowledged that "intentional discrimination" by attorneys for the three white defendants charged in the death of the Black man appeared to have shaped jury selection. But he said Georgia law limited his authority to intervene.

Race is a central issue in the case involving the death of Arbery. Greg McMichael and his adult son, Travis McMichael, armed themselves and pursued Arbery in a pickup truck on February 23, 2020, after they spotted the 25-year-old man running in their neighborhood in coastal Georgia. A neighbor, William "Roddie" Bryan, joined the chase in his own truck and took cellphone video of Travis McMichael shooting Arbery three times with a shotgun.

A long, sometimes heated debate over the racial makeup of the final jury erupted in court Wednesday afternoon as lawyers wrapped up a jury selection process lasting more than two weeks.

Arbery's death became part of the broader reckoning on racial injustice in the criminal legal system after a string of fatal encounters between Black people and police — George Floyd, Breonna Taylor and Rayshard Brooks, among others.

No one was charged in Arbery's death until more than two months afterward, when the video of the shooting leaked online. The Georgia Bureau of Investigation took over the case from local police and soon arrested all three men on charges of murder and other crimes.

Minutes after the attorneys had finished narrowing a panel of 48 to a final jury of 12 on Wednesday, prosecutor Linda Dunikoski noted only a single Black juror made the panel.

She argued that defense lawyers had struck eight Black potential jurors because of their race. The U.S. Supreme Court has held that it is unconstitutional for attorneys during jury selection to strike potential jurors solely based on race or ethnicity.

Laura Hogue, an attorney for Greg McMichael, insisted those jury panelists were cut for other reasons — namely for expressing strong opinions about the case when questioned individually by attorneys.

"I can give you a race-neutral reason for any one of these," Hogue said.

She noted one such juror had written on her juror questionnaire that Arbery was shot "due to his color" and had told attorneys she felt the defendants were guilty.

Superior Court Judge Timothy Walmsley denied prosecutors' request to reinstate those eight Black potential jurors, though he said: "This court has found there appears to be intentional discrimination in the panel."

The judge said his ability to change the jury's racial makeup was limited because defense attorneys were able to give nonracial reasons for their decisions to strike the potential Black jurors.

"They have been able to explain to the court why besides race those individuals were struck from the panel," Walmsley said.

The judge said the jury, along with four alternates, will be seated and sworn in Friday, when opening statements in the trial are expected. He did not give the races of the alternate jurors.

Arbery's mother, Wanda Cooper-Jones, told reporters outside the courthouse she found it "devastating" that only one Black juror will be seated. Still, she said of the final jury: "I'm very confident that they'll make the right decision after seeing all the evidence."

Her attorney, S. Lee Merritt, said he still believes the trial will end in a conviction, though defense lawyers had "created a jury that was more favorable for their defendants, an almost entirely white jury."

	Dunikoski noted that many prospective jurors questioned in open court expressed strong opinions about the case, but all who remained in the pool from which the 12 jurors emerged said they could be impartial and base a verdict solely on the trial evidence. In Glynn County, where Arbery was killed and the trial is being held, Black people account for nearly 27% of the population of 85,000, according to the U.S. Census Bureau. The judge said 25% of the pool from which the final jury was chosen was Black. Defense attorneys say the McMichaels and Bryan committed no crimes. They say Arbery had been recorded by security cameras inside a nearby house and they suspected him of stealing. Greg McMichael told police his son opened fire in self-defense after Arbery attacked with his fists and grappled for Travis McMichael's shotgun. Investigators have said Arbery was unarmed and there's no evidence he had stolen anything. The slaying dominated news coverage and social media feeds in Glynn County, about 70 miles south of Savannah. That caused court officials to take extraordinary steps in hopes of seating an impartial jury. They mailed 1,000 jury duty notices, and nearly 200 people were questioned by the judge and attorneys at the courthouse during jury selection.
Return to Top	

Information From Online Communities and Unclassified Sources/InFOCUS is a situational awareness report published daily by the Washington State Fusion Center.

If you no longer wish to receive this report, please submit an email to intake@wsfc.wa.gov and enter UNSUBSCRIBE InFOCUS in the Subject line.

Return to Top