Washington State Fusion Center
INFOCUS
WEDNESDAY – 8 NOV 2017

	International	National	Regional and Local
Events, Opportunities Go to articles	11/08 Philippines backs down in S. China Sea 11/08 Protesters disrupt transit in Catalonia 11/08 NKorea officials: done listening to US 11/08 India lauds last year's rupee swap 11/07 India air 'public health emergency' 11/07 Saudi crown prince blames Iran 11/07 Buddhist nationalism regional reach	11/08 Election night roundup top US races 11/07 How rich stay rich by hiding wealth 11/07 IG reports: DHS has key vulnerabilities 11/07 Puerto Rico needs 'unprecedented' help 11/07 New CPR guidelines for dispatchers, kids 11/07 Claim: Red Cross floundered Harvey relief 11/07 Experts: mass shootings getting deadlier 11/07 Church security scrutinized after killings 11/07 Vegas steps up security for rock festival 11/07 Record 456tons unused pills collected 11/07 Subsidized sex assault 'hush money' 11/07 Baltimore cop cleared in Gray case 11/07 Report: ACA signups surge 11/06 San Diego hepatitis outbreak grows	11/07 More snow coming to Cascades 11/07 Seattle election night takeaways 11/07 King Co. voters approve more taxes 11/07 Jenny Durkan wins Seattle mayor race 11/07 King Co. sheriff trails in reelection race 11/07 Uncle in Kelso messaged Texas shooter 11/07 Seattle police museum closing; moving 11/07 Yakama Nation sues Klickitat County 11/07 FBI raids HQ body broker firm
Cyber Awareness Go to articles	11/08 Russia-linked spies exploit DDE 11/07 'Sowbug' stealing diplomatic secrets 11/07 Flaw locks out $300M cryptocurrency 11/07 Drive-by cryptomining hassles visitors 11/07 Canada police frustration w/cybercrime 11/07 Marcher banking Trojan targets Austria 11/07 Shipping faces expanding cyber threats 11/07 Scottish charity leaks data on vulnerable 11/07 Study: most firms run old Office software 11/07 Expert: cyber threat to UK railways is real 11/07 Cost cybercrime rising; attacks increasing	11/08 FBI: church shooter's phone 'locked' 11/07 Report: DHS cyber intel sharing falls short 11/07 Growing threat synthetic identity fraud 11/07 Hackers exploit New York terror attacks 11/07 Pro-ISIS hackers hijack school websites 11/07 Downloading fake apps; getting hacked 11/07 Charities unprepared in cyberattack risk 11/07 Texas Nat'l Guard $373,000 on stingray 11/07 Experts: threats to satellites are legion 11/07 New technology cyber threats aviation 11/07 Gaming keyboard w/built-in keylogger 11/07 Twitter doubles character limit to 280 11/07 Phony Netflix email phishing scam 11/07 Electric industry facing cyber alert 11/07 Lessons from critical infrastructure 11/06 What happened to GozNym Trojan?	
Terror Conditions Go to articles	11/08 ISIS turns to social media for support 11/08 West Africa force faces uphill battle 11/07 NATO send more troops to Afghanistan 11/07 French-Swiss anti-terror sweep nets 10	11/07 Bin Laden son seeks revenge against US 11/07 Doctor denies financing NY bomb plots 11/07 Airstrikes on ISIS targets drop 60%	
Suspicious, Unusual Go to articles	11/07 Mexico military abuses go 'unpunished' 11/07 Dementia now Britain's biggest killer 11/07 NASA: volcanic activity Antarctica	11/07 Pentagon: known USAF 'systemic issue' 11/07 Pentagon known crime reporting lapses	11/07 State's first wildlife K9 officer
Crime, Criminals Go to articles	11/08 China: UCLA basketball players arrested 11/08 Japan yakuza struggle to earn a living	11/07 Ohio busts 100 in fentanyl drug ring 11/07 Penn. trooper shot during traffic stop 11/07 Air Force: Tex. shooter 'serious problem' 11/07 Strangers acted together to stop shooter 11/07 Claim: gunman deliberately shot babies 11/07 Domestic violence, mass killings link? 11/07 Shooter escaped mental facility 2012 11/07 Assault rifle role in mass shootings 11/07 Latest on Texas church shooting	11/07 Man set on fire in north Seattle

Event Calendar

Top of page

Date	Event	Location/Time	Other Information
9-13 Apr 2018	LEIU/IALEIA Training Event	Marriott Hotel, 700 West Convention Way	http://www.ialeia.org/2018_conference.php

		Anaheim, CA 92801 (714) 750-8000
Return to Top	**indicates new event/new information added during reporting week	

Events, Opportunities

Top of page

HEADLINE	11/07 Jenny Durkan wins Seattle mayor race
SOURCE	http://www.king5.com/news/local/seattle/jenny-durkan-wins-seattle-mayors-race-over-cary-moon/490001440
GIST	Jenny Durkan won the race for Seattle mayor Tuesday in one of the most competitive mayoral races in recent Seattle political history. The history-making race also produced the city's first female mayor in 91 years. Durkan took a big lead over Cary Moon after initial returns were released Tuesday, earning 60.62 percent of the vote (64,174 votes). Moon trailed with 39.38 percent (41,683 votes). About 105,000 votes were counted Tuesday night. "There's a lot of votes left to be counted, but…we are feeling really, really good about where we are, and I think you guys should celebrate," Durkan told supporters at her election party Tuesday. Moon acknowledged her campaign was "up against tough odds" after initial returns were released, but said she was not giving up hope. "Seattle late voters may surprise everyone," Moon said in a statement. "We believe the ballot counts will swing in our direction over time, and we're not out of the race yet." Durkan served as U.S. Attorney for Western Washington under President Barack Obama. In that role, Durkan helped negotiate the current consent decree that forced ongoing reforms at the Seattle Police Department. The Seattle native, a graduate of Notre Dame and UW Law School, earned a reputation as a formidable litigator before being picked in the first wave of Obama's U.S. attorney appointments.
Return to Top	

HEADLINE	11/07 How rich stay rich by hiding wealth
SOURCE	https://www.nytimes.com/2017/11/07/world/offshore-tax-havens.html
GIST	James H. Simons, a reserved mathematician and hedge fund operator from Boston now approaching 80, is a big Democratic donor. Warren A. Stephens, a 60-year-old golf enthusiast once called the king of Little Rock, Ark., inherited a family investment bank and became a booster of conservative Republicans. But Mr. Simons and Mr. Stephens are both billionaires who have used the services of offshore finance — the trusts and shell companies that the world's wealthiest people use to park their money beyond the reach of tax collectors and out of the public eye. Mr. Simons was the main beneficiary of a private trust, never previously described, that was one of the largest in the world. In response to recent questions about the trust, Mr. Simons said that he had transferred his share to a Bermuda-registered charitable foundation. Mr. Stephens used an opaque holding company to own an approximately 40 percent stake in a loan business accused by the federal Consumer Financial Protection Bureau of cheating working-class and poor Americans. While earning millions from the investment, Mr. Stephens helped finance a political onslaught

against the bureau, never mentioning his personal connection to the fight.

The details of the two men's hidden wealth come from the files of Appleby, founded in Bermuda more than a century ago and considered one of the world's top offshore law firms. A collection of 6.8 million Appleby documents, obtained by the German newspaper Süddeutsche Zeitung and shared with media organizations through the International Consortium of Investigative Journalists, offers an inside look at the firm's services and customers.

Appleby operates in a rarefied universe of ultra-high-net-worth individuals, where yachts and private jets are preferred transport and mansions sit empty because their owner has several others. Some of Appleby's customers are also P.E.P.'s — politically exposed persons — for whom avoiding unwanted attention is a crucial goal.

"The Right People. The Right Places," reads the slogan on Appleby's stationery.

What offshore services offer to a diverse international elite is secrecy and discretion, along with the opportunity to minimize or defer taxes. Appleby appears to be more scrupulous than another offshore firm, Panama-based Mossack Fonseca, about shunning overtly corrupt and criminal clients, based on a comparison of the Appleby files with the leaked Panama Papers, which drew global coverage last year.

Appleby board minutes contain lists of "declined business," including government officials suspected of corruption and millionaires linked to organized crime.

Still, some dubious clients slip through. A PowerPoint slide used by Appleby's head of compliance discusses terrorist financing and refers to funds that were "definitely tainted."

"Some of the crap we accept is amazing totally amazing," say notes to a slide about sizing up potential customers.

Even with some potential customers turned away, business has rarely been better. The ranks of the superrich are growing fast, fueled by legitimate fortunes in finance, trade and technology — as well as drugs, embezzlement and bribery. And the offshore finance industry has grown alongside its customers' accounts.

The global number of wealthy people with more than $50 million in assets is about 140,900, half of them in the United States, according to a recent report from Credit Suisse.

A 2015 Appleby publication written for such clients, "Wealth Structuring 20:20," features photos of a handsome couple and their children hurrying to board a sleek personal jet. "Wealth seeks out safe harbours," one article is titled. Another advises on "Motivating children of means."

In emails, Appleby employees fret about how to pamper well-heeled clients.

"Our fees are around 40k and they are the sort of people who I think would appreciate popping a bottle on closing at Appleby this afternoon," a lawyer in the firm's Grand Cayman office wrote in 2008 of a particular deal. "Do you have the key to the booze vault? It would need to be decent stuff as they'll know their champagne."

The legal boilerplate in the leaked documents can be eye-glazing until, as in a 2015 financing agreement, you discover that the deal is for a spectacular $50 million yacht, the Galactica Star, that Jay-Z and Beyoncé once borrowed for a vacation.

Appleby had 31,000 American clients, the most common nationality by far. The firm's files include a who's who of the nation's wealthiest citizens: prominent Democrats like George Soros, the financier and philanthropist, and Penny Pritzker, commerce secretary in the Obama administration; and high-profile Republican supporters of President Trump, including Sheldon Adelson, the casino magnate, and Carl

	Icahn, the private equity investor. Queen Elizabeth II, according to Appleby documents, used a Cayman Islands fund to invest in a company that owned a share of a British rent-to-own company widely criticized for financing the sale of household items at interest rates as high as 99.9 percent. The leaked files reveal Madonna's shares in a medical supplies firm, Bono's investment in a Lithuanian shopping center and the Microsoft co-founder Paul G. Allen's yacht and submarines. Around the globe, the documents disclose the holdings of rulers and politicians. The list includes three former prime ministers of Canada, the queen dowager of Jordan and at least five members of the Qatari ruling family. Another offshore firm, the family-owned Asiaciti of Singapore, whose files were obtained by Süddeutsche Zeitung, advertises that it helps clients "preserve wealth from the ravages of litigation," political tumult and divorce. Its American customers include physicians, professional poker players and a Colorado alfalfa farmer. Asiaciti set up trusts in the Cook Islands for Kevin Trudeau, an infomercial pitchman in the United States with a trail of legal troubles who sold millions of copies of such self-help books as "The Weight-Loss Cure 'They' Don't Want You to Know About." Founded in 1898 by a British officer, Maj. Reginald Appleby — an avowed opponent of taxation — Appleby now has offices in nearly all the world's tax havens: Bermuda, the British Virgin Islands, the Cayman Islands, Guernsey, Hong Kong, the Isle of Man, Jersey, Mauritius, the Seychelles and Shanghai. Such locations offer low or zero tax rates, companies consisting only of a postbox, and accountants and lawyers skilled at hiding money. In a statement, Appleby said the firm had done nothing wrong. "We are an offshore law firm who advises clients on legitimate and lawful ways to conduct their business," the statement said. "We do not tolerate illegal behaviour." In recent years, billionaires' fortunes have grown by an average of 7 to 8 percent a year, while total wealth has grown at just 3 percent annually, said Gabriel Zucman, an economist at the University of California, Berkeley. Globalization, deregulation and declining taxes have all been factors. "The other important thing is the rise of the global, cross-border wealth management industry," including Appleby, Mr. Zucman said. The richest 1 percent of the world's population now owns more than half of global wealth, and the top 10 percent owns about 90 percent. "The data suggests that most of the gains at the top are coming at the expense of the rest of the population," Mr. Zucman said. That conclusion is shared by many other scholars. The wealthy use the power that accompanies their money, he said, to exert political influence, reduce taxes and regulation — and hire experts to keep their money safe.
Return to Top	

HEADLINE	**11/07 IG reports: DHS has key vulnerabilities**
SOURCE	**https://www.usatoday.com/story/news/politics/2017/11/07/homeland-security-lost-guns-backlogged-asylum-application-vulnerabilities-lax-grant-oversight-dhs/838089001/**
GIST	WASHINGTON — The Department of Homeland Security has key vulnerabilities in administration and oversight that could leave the agency open to fraud and pose threats to national security and public safety, according to a series of reports issued in recent weeks by the department's inspector general.

The problems range from miscommunications on immigration to oversight failures at the Federal Emergency Management Agency and a skyrocketing backlog of asylum applications that could present a "significant risk to national security and public safety," the inspector general found.

The issues show just how steep the challenges are for President Trump's pick to lead the agency, Kirstjen Nielsen, who is facing a Senate confirmation hearing Wednesday.

The 15-year-old agency, created to help keep Americans safe after the 9/11 terrorist attacks, has a broad mission guarding the nation's ports, borders and airports and overseeing federal disaster response and recovery.

Nielsen is an attorney with homeland security and cybersecurity experience who was chief of staff to Gen. John Kelly at DHS before he became White House chief of staff. She followed him to the White House, where she is principal deputy chief of staff. Previously, she worked at the Transportation Security Administration and on the White House Homeland Security Council under President George W. Bush.

Here are some of the key vulnerabilities identified by the DHS inspector general — and issues she faces if confirmed.

Asylum backlog

A backlog of asylum applications has skyrocketed in recent years, jumping from roughly 57,000 in 2014 to more than 250,000 this year.

Immigrants who are already in the United States can seek asylum by filing an application with U.S. Citizenship and Immigration Services, which then reviews them and sets up fingerprinting, background checks and interviews before asylum can be granted.

The inspector general did not indicate where in the process the backlogged applications are, but the IG's office told USA TODAY that USCIS officials indicated they had only received initial, preliminary vetting.

"These cases present a significant risk to national security and public safety when not vetting the applicants' backgrounds," the inspector general concluded.

Eliminating the backlog without added staffing or policy changes could take years, and in the meantime, the inspector general said, USCIS officials have identified fraud trends in the program.

"Individuals may file for affirmative asylum, anticipating a prolonged waiting period, as a means of exploiting the application process to obtain an Employment Authorization Document," the inspector general said.

Last year, the department implemented an "asylum surge issue team" to help improve processing, but the inspector general found "no meaningful changes implemented."

Immigration miscommunications

DHS does not foster enough coordination between its offices responsible for immigration administration and enforcement, which has led to miscommunications and breakdowns, the inspector general found.

The inspector general identified issues with bed space availability, inmate transfer responsibility, language services and processing of undocumented immigrants because of different decisions made by U.S. Customs and Border Protection, U.S. Immigration and Customs Enforcement and U.S. Citizenship and Immigration Services.

CBP apprehends immigrants but relies on ICE to house them, yet ICE didn't consistently notify CPB if and where beds were available. In addition, while CBP is a 24-hour, seven-day operation, ICE

enforcement and removal staff normally don't work nights and weekends, leaving customs and border workers scrambling to house detainees.

A decision by USCIS last year to stop conducting interviews with individuals not currently detained at one location prompted ICE to convert nearly 2,000 cases pending asylum hearings to notices to appear in court. An ICE official said they likely would have been removed and not released into communities if their cases had been adjudicated upon entry to the United States.

ICE officials also didn't always communicate with USCIS when they moved or released detainees, so USCIS at times showed up at facilities to do interviews but the subjects were not there.

"Lack of coordination in processing aliens creates potential vulnerabilities to national security and public safety," the inspector general found.

In response to the report issued last week, department officials said they planned to establish a policy council with members from ICE, USCIS, CBP, and other offices to coordinate department-wide administration of immigration policies.

Hundreds of guns, badges lost

Between 2014 and 2016, DHS personnel lost thousands of sensitive assets including guns, badges and secure immigration stamps, the inspector general found.

Border patrol, ICE agents and TSA officers are among DHS personnel who carry guns and badges that pose a security risk if they are lost or stolen. A total of 228 guns and nearly 1,900 badges went missing during the two-year period.

The IG cited instances where two off-duty ICE officers left guns in backpacks while on a beach in Puerto Rico, and another left his gun and badge unsecured in a hotel room while on vacation.

A CBP officer left his badge in an unlocked public gym locker, another left his gun in a bag at a friend's house, and a third left his gun in an unlocked car overnight. A TSA officer left his gun in his car while he had dinner with his family.

All were stolen.

Only a fraction of the officers were disciplined and none received remedial training on safeguarding such sensitive assets in the future.

In three cases, the inspector general found, weapons fell into the hands of convicted felons.

"Police recovered one firearm from an individual in possession of heroin; another from a suspect charged with armed robbery; and the last from a convicted felon at a pawn shop," the IG wrote.

DHS officials said they concurred with the findings and plan to update policies, training and inventory control for guns and badges.

Marshaling better aviation security

The contribution to aviation security of the Federal Air Marshal Service is "questionable," the inspector general concluded.

The details of the findings are classified but an unclassified summary said investigators made five recommendations for improvement. "We also identified a part of FAMS operations where, if discontinued, funds could be put to better use," the summary states.

	Part of the Transportation Security Administration, the service deploys marshals on commercial flights to "protect airline passengers and crew against the risk of criminal and terrorist violence." But critics contend that there are only enough marshals to cover 5 percent of flights, and yet the program accounts for 10 percent of the TSA's budget, costing more than $800 milion per year. "In general, spending one dollar on the service generates less than 10 cents in benefit," wrote John Mueller, a political scientist at the Cato Institute and Ohio State University, and Mark Stewart, a civil engineer and risk analyst at the University of Newcastle in Australia. Mueller told USA TODAY he believes they are virtually useless. "They do nothing," Mueller told USA TODAY in an interview. "They may have helped with a few drunks here and there. They've apprehended nobody." Mueller and Stewart, co-authors of Are we safe enough? Measuring and assessing aviation security, maintain that slashing the marshal service's budget by 75%, increasing training and arming of pilots and installing secondary barriers to cockpits would produce "better aviation security and a savings of hundreds of millions of dollars each year." **Disastrous loan oversight** In a separate report released last month, the inspector general found that FEMA "did not manage disaster relief grants and funds adequately and did not hold grant recipients accountable for properly managing disaster relief funds." Between 2009 and 2015, the inspector general identified $1.6 billion in questionable costs. Last year, the watchdog found another $155 million. They included instances where projects did not qualify or grant recipients did not ensure full and open competition for work under the grants, did not provide opportunities to small, women- or minority-owned business and used prohibited cost-inflated contracts. FEMA provides grants to state and local governments and nonprofit organizations to help response and recovery from major disasters. The inspector general also audited the agency's initial response to major disasters and found the responses were effective but noted "FEMA's management responsibility merely begins with the initial disaster response." In response to the report, FEMA officials said they are committed to addressing the findings and the agency is working to advance consistent, FEMA-wide guidance for grant management and compliance.
Return to Top	

HEADLINE	**11/08 Election night roundup top US races**
SOURCE	**https://apnews.com/692af57eb88f44be9d4cc42d05395ccf/A-look-at-the-winners-and-losers-of-the-top-US-races**
GIST	Democrats swept Virginia and New Jersey's governor's races, incumbents came out on top in several big-city mayoral races and voters in Maine said they wanted to join 31 other states in expanding Medicaid under the Affordable Care Act. A rundown of the top races around the country on Tuesday: TWO GOVERNORS

Voters in two states picked replacements for their term-limited governors — Democrat Terry McAuliffe in Virginia and Republican Chris Christie in New Jersey — in contests seen as an early referendum on the presidency of Donald Trump. In swing state Virginia, Democratic Lt. Gov. Ralph Northam defeated Republican Ed Gillespie. In New Jersey, front-running Democrat Phil Murphy overcame Republican Lt. Gov. Kim Guadagno.

The stakes were high as both parties sought momentum ahead of next year's midterm elections. Democrats haven't won any special elections for Congress this year and the next Virginia governor will have a major say in the state's next round of redistricting, when Congressional lines are drawn. Republicans were looking for a boost as their party is beset by intraparty turmoil between Trump and key Republicans in Congress.

BIG-CITY MAYORS

Democrat Bill de Blasio won a second term as mayor of heavily Democratic New York City. He easily defeated Republican state lawmaker Nicole Malliotakis and several third-party candidates.

In Boston, Mayor Marty Walsh won a second four-year term by beating City Councilor Tito Jackson after a low-key campaign.

Detroit Mayor Mike Duggan won a second four-year term by defeating state Sen. Coleman Young II, whose father was the city's first black mayor. Duggan was first elected after a state-appointed manager filed for Detroit's historic bankruptcy.

Two Atlanta city councilwomen, Keisha Lance Bottoms and Mary Norwood, were the top two vote-getters in the city's mayoral race from a field of nearly a dozen candidates and are now headed to a Dec. 5 runoff. The winner will replace term-limited Atlanta Mayor Kasim Reed.

In Seattle, former U.S. Attorney Jenny Durkan took a strong early lead in the race for mayor. Voters were choosing between Durkan and urban planner Cary Moon to replace former Mayor Ed Murray, who resigned earlier this year amid sexual abuse allegations. Ballot counting in the all mail-in election will continue over the next several days.

Charlotte, North Carolina, is getting its sixth mayor since 2009. Mayor Pro Tem Vi Lyles, a Democrat, beat Republican City Councilman Kenny Smith.

MEDICAID

Maine voters approved a measure allowing them to join 31 other states in expanding Medicaid under the Affordable Care Act. The referendum represented the first time since the signature health bill of former President Barack Obama took effect that the question of expansion was put before U.S. voters. Maine's Republican governor had vetoed five attempts to expand the program.

UTAH'S CONGRESSIONAL SEAT

The Republican mayor of the Mormon stronghold of Provo, Utah, won a special election to replace U.S. Rep. Jason Chaffetz, who resigned earlier this year. In an expected victory in the heavily Republican congressional district, John Curtis beat Democrat Kathryn Allen and third-party candidate Jim Bennett.

PHILADELPHIA DISTRICT ATTORNEY

Philadelphia's next district attorney is Larry Krasner, a liberal Democrat who vows to end mass incarceration and the death penalty. He replaces Democrat Seth Williams, who was sentenced to prison last month for accepting a bribe.

	CONTROL OF WASHINGTON Democrat Manka Dhingra took an early lead in a state Senate race that will determine whether the Washington state Senate will remain the only Republican-led legislative chamber on the West Coast. If the seat flips to Democrats , Washington will join Oregon and California with total Democratic rule in both legislative chambers and the governor's office. Under the state's vote-by-mail system, ballots just need to be postmarked or dropped off by Tuesday, which means that final results may not be known for days.
Return to Top	

HEADLINE	**11/07 Buddhist nationalism regional reach**
SOURCE	**https://www.usnews.com/news/best-countries/articles/2017-11-07/buddhist-nationalism-reaches-beyond-myanmar**
GIST	As hundreds of thousands of Rohingya flee across the border from Myanmar to Bangladesh, stories of terror and suffering continue to mount: tales of torched villages and gang rape, of soldiers stabbing babies and cutting off heads. U.N. human rights chief Zeid Ra'ad al-Hussein has called the violence – allegedly committed by Myanmar's security forces and local mobs – "textbook ethnic cleansing." In the case of Myanmar, a Buddhist-majority country, the attacks are fueled by a radical form of Buddhist nationalism. While most of the world's Buddhists would never condone such extremism, violence in the name of the faith has a long history, experts say. Yet for many people, images of monks in saffron robes inciting riots seem counterintuitive. "In popular culture and many academic works, Buddhists are not known as violent or advocates of conflicts or wars," says Michael Jerryson, a professor of religious studies at Youngstown State University. "Rather, Buddhists are presented as pacifists. In this way, the vast and diverse world of over 1.3 billion people who practice Buddhist rituals are collectively associated with meditation and tranquility." That can be chalked up to a mix of factors, Jerryson says, including how Buddhism was first introduced to the U.S., the Free Tibet campaign and the influence of the beatnik movement and Hollywood. Though the killing in Myanmar, the Southeast Asian nation formerly known as Burma, is grabbing headlines, it's actually one of several primarily Buddhist countries where nationalists are encouraging violence. Here are the ones that should be on your radar: Myanmar More than 600,000 Rohingya Muslims have fled to Bangladesh since late August, when Myanmar's security forces launched an operation which rights groups say involved mass atrocities in the western state of Rakhine. The government says the crackdown was in response to attacks by Rohingya militants on a military camp and security forces outposts. The military claims it was only targeting insurgents, yet, according to witnesses who spoke to The New York Times, many of those killed were unarmed and had their hands bound. While the campaign in Rakhine state has significant public support, many Buddhists reject the violence in other parts of the country against Muslims, whom Buddhists may not accept as indigenous but acknowledge as Myanmar citizens. Buddhist nationalism in Myanmar, like in many parts of Southeast Asia, can be traced to a complex set of circumstances, including bouts of significant political or economic upheaval that have left some Buddhists feeling threatened. Most scholars attribute its rise in part to British colonialism, during which Buddhism was forcibly separated from the state, and the government facilitated the immigration of Indian moneylenders and landholders – Hindus and Muslims – angering local elites. "The Burmese have a long history of saying 'To be Burmese is to be Buddhist' and for the most part that

model, that vision has endured since independence," says Juliane Schober, director of the Center for Asian Research at Arizona State University.

Myanmar's recent spike in Buddhist nationalism and anti-Muslim sentiment took off after the country's military junta dissolved in 2011, according to a recent report by the International Crisis Group, a Washington, D.C.-based nonprofit group dedicated to preventing conflict. In 2013, Buddhist monks incited mob violence against Muslims that left more than 20 dead.

The Association for the Protection of Race and Religion, also known as MaBaTha, is the most well-known of the country's ultra-nationalist groups. While the government has tried to crack down on the organization, which is known and respected by many for providing social services, it has had limited success.

Some members of the group, made up of monks, nuns and laypeople, believe Myanmar's Muslims are "hoarding capital, buying up real-estate in town centres, using their wealth to woo and marry Buddhist women, then forcing their wives and children to convert to Islam through physical or economic pressure," according to the ICG report.

Sri Lanka

On June 15, 2014 anti-Muslim riots broke out in the Sri Lankan coastal town of Aluthgama. For two days, rioters desecrated and damaged mosques and burned and looted hundreds of Muslim-owned houses and businesses. At least 80 people were injured and four died in the worst anti-Muslim violence in almost a century.

The perpetrators? Sinhalese Buddhists, likely inspired by a radical monk who spoke violently against Muslims during a rally shortly before the attacks.

Since 2012 – about the time Buddhist nationalism was gaining steam in Myanmar – militant Buddhists in Sri Lanka began using hate-speech and violence against Muslim and Christian minorities. The most well-known of the groups is the Bodu Bala Sena, or Buddhist Power Force, an organization among several that has close ties to Myanmar's militant Buddhists.

While Buddhist attacks on Muslims virtually disappeared after Sri Lanka's current government was elected in 2015 – in part due to overwhelming support from Muslim voters – "2017 has seen a worrisome return of violence and hate speech," says Alan Keenan, Sri Lanka senior analyst for ICG. He worries that events in Myanmar, and the impunity with which Muslims have been killed and expelled from the country, "could further empower radical Buddhists groups in Sri Lanka."

Although that might already be happening. In September, a mob led by Sri Lankan Buddhist monks stormed a U.N. shelter for Rohingya Muslims on the outskirts of the capital, demanding that they be sent back to Myanmar.

Buddhist nationalism has long been a political force in Sri Lanka, an island nation off the southern coast of India. While Sinhalese Buddhists make up about 70 percent of the country, many believe Buddhism and Sinhalese identity are under threat. The Sri Lankan constitution gives Buddhism the "foremost place" in the nation, and the nationalist cause was often invoked during the country's nearly 30-year civil war with the Tamil Tigers, most of whose fighters came from the Tamil, mostly Hindu minority.

After the end of the war in 2009, attention turned toward Muslims, who make up about 10 percent of the country. Like in Myanmar, some nationalistic Buddhists worry that Muslims will outpace them in population growth and marry and convert their women. Some Sri Lankans, along with some like-minded Buddhists in Myanmar and Thailand, also share the belief that Theravada Buddhism – the form of Buddhism practiced in those countries – is under threat from a powerful global Islamic community, says Keenan.

	Thailand While anti-Muslim sentiment in Thailand has some overlapping roots with Sri Lanka and Myanmar, it can also be attributed to another force: an ongoing Muslim separatist movement. For about 13 years, Malay-Muslim militants have been waging an insurgency in the country, where about 95 percent of the population is Buddhist. For most of that time, the conflict, which has killed around 7,000 people, has been limited to Thailand's southernmost provinces – the area which militants consider to be their historical homeland. But in 2016 they expanded their campaign well beyond the deep south, targeting resort areas. The southern insurgency angers many Buddhist nationalists in Thailand, a dynamic that has potential to fuel sectarian conflict, says Matt Wheeler, senior Southeast Asia analyst with ICG. In 2015, Buddhists held large protests against a halal-industry zone and the construction of a new mosque in the north, he notes. And in October of 2015, a since defrocked monk in Bangkok grabbed headlines after calling on his social media followers to burn a mosque for every monk killed in the south – a move, according to Newsweek, that only attracted more followers. Social media isn't only being used to fan the flames of Buddhist nationalism in Thailand. Experts say radical Buddhist nationalists in all three countries have begun to connect on the internet to a worrying degree – swapping conspiracy theories and mimicking each other's fiery rhetoric.
Return to Top	

HEADLINE	**11/07 Seattle police museum closing; moving**
SOURCE	**http://crosscut.com/2017/11/bertha-may-have-dealt-a-blow-to-seattles-police-museum/**
GIST	The Seattle Metropolitan Police Museum, one of the historic gems of Pioneer Square, has announced that it is closing and moving its collection due to safety concerns. The museum, located near Third Avenue South and Jackson Street, is devoted to the history of the Seattle Police Department and the King County Sheriff's Department. The man in charge and the museum's guiding spirit is SPD Officer Jim Ritter. He says he believes the building has become untenable for his museum due to ground settling and visible cracks that he suspects are due to Bertha and the waterfront tunnel project. Ground settlement has been a big issue in Pioneer Square, much of which is built on landfill and former mudflats. The city had to contend with replacing a major sewer line on First Avenue due to settlement. Buildings near the Bertha tunnel boring machine rescue pit were also at risk. Other property owners have filed claims with the state over tunnel project-related damage. Ritter says some of the building's floorboards have rotted due to damage from a steam tunnel break. One of the museum board members put her high heel right through the rotten floorboards, he says. Some of the damage is very visible: The sidewalk outside is sloping. Cracks have appeared in the original 1909 plaster walls of the building, but also in newer drywall. One of the original brick walls appears to be bowing. Many of the doors that Ritter installed himself can no longer be closed properly. All of this damage, he says, has occurred in the last 18 months to two years. Ritter emphasizes that he's no engineer, but from a layperson's perspective, he's very concerned. The building has survived several major earthquakes and Ritter can point to some old scars from the 1965 and 1949 Seattle earthquakes. Also, part of the facade collapsed during the 2001 Nisqually quake, but that was repaired and the building was deemed sound after that. Since there hasn't been a major quake in the

	last 18 months, but tunnel and seawall work has taken place, "when you start looking, you can make a circumstantial case" for Bertha, he says. The building is owned by the Samis Land Company, which owns 11 properties in Pioneer Square, according to Adam Hasson Samis' director of real estate. Hasson says Samis has seen some damage at its other properties, but mostly cosmetic damage — some drywall cracking or stick door jams, "not anything dangerous," he says. Samis has not yet filed any claims with WSDOT for tunnel-related damage. An engineer will inspect the museum's space this week to determine whether there's a true safety risk. Ritter says Samis has been very good to the museum and gave them a break on rent that enabled them to afford the space. The museum was facing a rent increase, but Ritter says that's not the main reason for the move. He wants to ensure the safety of the museum's one-of-a-kind-collection and its patrons. All of SPD's history could be gone if there were a major problem or collapse in a quake, he says. His opinion is informed by experience: The museum only has one document on exhibit dating from before 1889 because virtually all of the city's police records were destroyed in the Great Seattle Fire. Ritter says the extensive collection, which includes uniforms, records, photographs, badges, weapons and other artifacts, will be placed in storage, but that won't be the end of the museum. He hopes to also put much of the collection online for researchers, and the museum has an extensive collection of police vehicles from the 1940s on that are shown off at public events and parades. The museum is financed through a payroll deduction plan of law enforcement officers at the city and county.
Return to Top	

HEADLINE	**11/07 Seattle election night takeaways**
SOURCE	**http://crosscut.com/2017/11/seattle-election-america-five-takeaways-resistance/**
GIST	From brewpubs to ballrooms, roving on election night can yield insights beyond the numbers. Here are my five election-night takeaways. **Seattle status quo breathes a sigh of relief** On election night, the crowd at Jenny Durkan's election night party at the Westin's ballroom was filled with Seattle establishment figures — a former mayor, PR spinners, legislators, downtown business figures. Before results were announced few were willing to make an election prediction. The establishment was nervous: Since Mike McGinn's insurgency and Kshama Sawant's election, the conventional wisdom doesn't trust itself anymore. Former City Councilmember Jan Drago, sipping red wine, told me she's out of the prediction business. "The city has changed so much." Or not. Durkan's victory has the Seattle establishment breathing a huge sigh of relief. KEXP commentator and longtime columnist Geov Parrish says Durkan "will be Ed Murray's second term, only without the creep factor." **The Blue Wall** A year ago, Donald Trump's election triumph shocked Seattle, but immediately the city leaders announced themselves part of the Resistance. This year, by capturing the 45th Legislative district state senate seat, Democrat Manka Dhingra has put a key brick in what Senate leader Sharon Nelson of Spokane described to the New York Times as a "blue wall from the Canadian border to the Mexican border." That wall consists of California, Oregon and now Washington where Democrats will have control of the governorships and state legislatures in all three states. But the significance of that — while it makes a statement nationally as the West Coast forms a kind of progressive bulwark against Trumpism — is more than symbolic for folks in Washington. It could mean progress on funding education, healthcare, and a capital budget, says State Senator Reuven Carlyle of Seattle. What might we see now from Olympia? "I expect you will see the legislature responsibly, humbly

working on real issues impacting real people." In the face of Trump's ideology, he continues, "There's never been a time in generations that the state government has mattered more."

The blue brick Dhingra represents was purchased dearly. That was reflected in the result that Democrats sought and Republicans fought with a record $9 million in campaign spending for a single suburban Senate seat in Olympia!

Women are winners

Seattle has finally broken the Bertha Knight Landes curse, having elected our first woman mayor since Landes some 90 years ago. Or as a press release from the Gay & Lesbian Victory Fund announced, "Jenny Durkan to Become First Out Lesbian Mayor of Seattle," presumably not wanting to make any assumption about Landes' orientation. But the election was "a banner night for women candidates" according to Maggie Humphreys of the National Women's Political Caucus of Washington State.

Exultant was longtime Seattle political consultant Cathy Allen who has long been a major force for women in politics. She points out that overshadowed by the Seattle mayor's race is the fact that out of some 230 King County candidates for office, 40 percent were women, up from the usual 30 percent.

"Where there are 11 women mayors right now in our cities over 30,000 people, by tomorrow it might be 27 women mayors all over the state," she says. "When women talked about doing something more after the Women's March in January, many talked of running for office — realizing that women were just not as equal as we thought we were."

Challenges ahead?

Jenny Durkan will take over at City Hall with a host of challenges on her to-do list: homelessness, housing affordability, police reform and union negotiations, and possibly a property tax bomb. King County Assessor John Arthur Wilson predicts that the impact of the legislature's plan to fund education statewide could raise property taxes early next year as much as 20 percent or more in Seattle.

"Does Tim Eyman finally get his policy wet dream?" Wilson wonders. City Councilmember Mike O'Brien says money will need to be raised by the city for urgent needs, but this could coincide or clash with impending property taxpayer sticker shock.

The left-leaning council and the more centrist progressive mayor will have to work together through some tough and intractable challenges without, perhaps, the usual piggy bank to draw on.

Return to Top

HEADLINE	**11/07 Yakama Nation sues Klickitat Co.**
SOURCE	**http://mynorthwest.com/806821/yakama-nation-sues-klickitat-county-over-arrest/**
GIST	YAKIMA, Wash. (AP) — The Yakama Nation has filed a lawsuit in U.S. District Court against Klickitat County in an ongoing dispute over whether 95,000 acres in the area is within reservation boundaries. The Yakima Herald-Republic reports the lawsuit was filed Friday concerning the arrest and conviction of a tribal member that happened about 30 miles northwest of Goldendale — which the tribe says is within the reservation. Arguing that the area is on the reservation, the tribe is seeking an injunction against the county, preventing its authorities from arresting and prosecuting tribal members there. The county previously sued the U.S. Department of Interior in federal court asking for a boundary determination after the tribe over a year ago had much of its criminal and civil authority over tribal members on the reservation restored by the state and federal government.

	A federal judge dismissed that case.
Return to Top	

HEADLINE	**11/07 Report: ACA signups surge**
SOURCE	**https://www.cbsnews.com/news/affordable-care-act-obamacare-sign-ups-surge-report/**
GIST	Open enrollment figures under the Affordable Care Act or Obamacare are showing a surge in the number of participants compared with years past, according to a new report by the Washington Post. The Post, citing federal officials who spoke on the condition of anonymity, reports that more than 200,000 Americans chose a plan on November 1st, the first day open enrollment began -- more than double the number of participants who signed up on the first day of enrollment in 2016. While the administration has yet to release final figures, an official also said that more than 1 million people visited HealthCare.gov, the official federal website to enroll in Obamacare -- about a 33 percent increase in users compared to last year. The Post notes that the figures only capture a portion of the nation's overall enrollment figures. More than a dozen states and the District of Columbia run their own enrollment programs and do not use the HealthCare.gov site for enrollees. This year's open enrollment period comes at a particularly contentious time for health care as fewer choices in the exchange marketplace and recent cutbacks from the Trump administration, including ending important reimbursements and slashing consumer support, make for an uncertain market and confused customers.
Return to Top	

HEADLINE	**11/07 Experts: mass shootings getting deadlier**
SOURCE	**https://www.nbcnews.com/storyline/texas-church-shooting/mass-public-shootings-are-getting-deadlier-experts-say-n818176**
GIST	With the slaughter of 26 people at a Texas church on Sunday, two of the deadliest mass shootings in American history have taken place in the span of just over a month — and experts said these types of cases have gotten deadlier in recent years. “If we look at say the top seven in terms of how deadly they’ve been, five of the seven deadliest have been in the last 10 years,” said Grant Duwe, a criminologist and author of "Mass Murder in the United States: A History." Duwe, who is the research director for the Minnesota Department of Corrections, said that while the rate of mass public shootings has not really increased in the past few decades, these cases have recently gotten more severe — both in the number of victims killed and the number of victims wounded. Four of the five deadliest mass public shootings in U.S. history have occurred in the last five years: the attack at a music festival last month in Las Vegas (58); at a nightclub in Orlando, Florida, in 2016 (49); at Virginia Tech in 2007 (32); at Sandy Hook Elementary School in Newtown, Connecticut, in 2012 (27); and at the First Baptist Church on Sunday in Sutherland Springs, Texas (26). Duwe said his research revealed a grim statistic: “With 94 victims killed so far this year, 2017 has been the deadliest year for mass public shootings in American history,” he said. That research defines “mass public shooting” as four or more victims killed with a firearm in a 24-hour period in a public location that is absent of other criminal activity, such as gang violence or a robbery.

Duwe said his research goes back to the year 1900.

The FBI has defined “mass murder” as the killing of four or more people within one event, according to a Congressional Research Service report.

With the attack in Texas on Sunday, Duwe said, “it’s difficult to deny the fact that there has been an increase in the severity of mass public shootings."

The United States also has more mass public shootings than any other country in the world, according to Adam Lankford, a criminology professor at the University of Alabama wrote a recent study on mass shooters and firearms spanning 171 countries.

Lankford said his statistical analysis looked at a variety of factors, including mental health, firearm ownership rates, and homicide and suicide rates.

“It’s a mathematical model that decides what’s important, and in this case it was far and away the firearm ownership rate which explained why some countries had more mass shooters than others,” he said.

The study concluded that the “United States and other nations with high firearm ownership rates may be particularly susceptible to future public mass shootings, even if they are relatively peaceful or mentally healthy according to other national indicators.”

Lankford said it was “pretty disturbing” that two of the nation’s deadliest shootings had happened within the last 35 days, and while motivations varied in such attacks, research and evidence left behind by gunmen in previous cases have shown that "these shooters do influence each other."

“I guess what a lot of average citizens would wonder is, are they connected? Is this an aberration that we’ve had these two shootings in such short proximity of each other or not?” he said.

Lankford noted examples where gunmen had left manifestos writing that they had been influenced by previous mass shooters. For example, more than 30 subsequent shooters cited the 1999 Columbine high school gunmen as a source of inspiration, he said.

"So the concern is, each one of these individuals who commit such a deadly attack could be a role model for future attackers, and of course that can explain why things could get worse in terms of America," he said. "America has more potentially deadly role models than it did two days ago."

Sherry Towers, a research professor at Arizona State University who has studied the spread of contagious disease in populations, published a study on “contagion in mass killings and school killings” after she noticed reports of three school shootings in a 10-day period in 2014.

Using a statistical model, the study found "significant evidence that mass killings involving firearms are incented by similar events in the immediate past."

"The way it manifests itself is usually a clustering together in time more than you’d expect by mere random chance," Towers said.

Towers' study also found that higher gun ownership and availability of firearms in a state were also factors.

She agreed with Duwe that, while data did not show a significant upward trend in the frequency of mass public shootings from year to year, "there is a significant trend upward in casualty count."

Return to Top

HEADLINE	**11/07 Saudi crown prince blames Iran**

SOURCE	**http://www.cnn.com/2017/11/07/middleeast/saudi-iran-aggression-yemen/index.html**
GIST	(CNN)Supplying rebels in Yemen with missiles was a "direct military aggression by the Iranian regime," declared Saudi Crown Prince Mohammed bin Salman bin Abdulaziz on Tuesday. In his first direct statements regarding a thwarted missile strike on the Riyadh airport that occurred over the weekend, bin Salman laid the blame for the attempt at the feet of Iran's government, claiming it was "supplying its Houthi militias [in Yemen] with missiles." In comments reported by the Saudi Arabian official news agency SPA, the Crown Prince told British Foreign Secretary Boris Johnson that Iran's actions "may be considered an act of war against the Kingdom." A spokesman for Iran's foreign ministry dismissed Saudi Arabia's allegations over the missile strike as "false, irresponsible, destructive and provocative," the Iranian news agency Tasnim reported Monday. Bin Salman's remarks were the latest by the Saudi government accusing Iran of not only being behind the actions taken in Yemen, but also for its purported behavior in Lebanon. For the Saudis, there would now be "no more distinction between Hezbollah and the Lebanese government," Saudi minister for Gulf affairs Thamer al-Sabhan said Monday. Hezbollah "has become a tool of death and destruction against Saudi Arabia and participates in all terrorist acts in the Kingdom," the minister claimed. Because of this, Saudi Arabia will treat the Lebanese as "a government declaring war," al-Sabhan told al-Arabiya, the Saudi-backed broadcaster.
Return to Top	

HEADLINE	**11/07 Vegas steps up security for rock festival**
SOURCE	**https://www.wsj.com/articles/las-vegas-steps-up-security-ahead-of-marathon-rock-festival-1510063201**
GIST	Organizers of the first major outdoor festival to be held on the Las Vegas Strip since last month's mass shooting are moving key events and ramping up security in an effort to keep participants and spectators safe while creating an upbeat atmosphere. Next weekend's Rock 'n' Roll Las Vegas Marathon, where bands play on stages at regular intervals along the 26.2-mile route, had been slated to kick off with a starting-line concert by the Goo Goo Dolls—playing at the same grounds as the Route 91 Harvest music festival where a gunman killed 58 and injured at least 500. The '90s rock band will now play the night before the race at the Las Vegas Festival Grounds. Andy Walsh, a captain with the Las Vegas Metropolitan Police Department who is heading up marathon preparations, said the October Vegas shooting and last Tuesday's terrorist attack in New York informed law-enforcement decisions. "This year we're on that list of cities that have proven to be vulnerable to somebody who's determined to do something," he said. "We use that in planning and strategy for this event, and it will be part of all future events" The Rock 'n' Roll Marathon—actually a series of races, including a 5K, 10K, half- and full marathon over the weekend of Nov. 11-12—is expected to draw more than 50,000 runners and spectators. The event, now in its ninth year, is traditionally marked by a headliner concert before the start of the races, with stages featuring local bands playing at each mile of the route. This year, the first 2½ miles of the

	race—which stretches along the site of the shooting and past the "Welcome to Las Vegas" sign—will have no music and instead serve as an extended moment of silence. "In such close proximity to a tragic event, we didn't want to be hosting a kickoff celebration," said Josh Furlow, president of the Rock 'n' Roll Marathon Series. "But the drumbeat going through town is 'Vegas Strong,' so the first checkmark was: 'Yes, we're going to be doing the event and hosting athletes from all over the world.' " The new route isn't as spread out as in years passed, helping law enforcement concentrate resources. Capt. Walsh said 350 police officers will be present throughout the weekend, while 180 police vehicles as well as trucks and barricades will "harden the intersections and make it impossible for a vehicle to pass through." Surveillance cameras and sniper nests will be planted along the route, and a police helicopter will hover overhead at all times. Stages along the route will be equipped to alert the crowd with instructions in case of an emergency. And Mr. Furlow said runners will receive instructions before the event on how much time they will need to navigate increased security. Fewer than 100 runners have sought refunds since the Vegas attack, and registration is on par with previous years, said Dan Cruz, a marathon spokesman. The starting location for the marathon and half-marathon has also been moved, from outside the Mandalay Bay Resort & Casino, where the gunman shot from the 32nd floor, to outside the New York-New York Hotel and Casino, about a mile up the road. Access to the starting line will be restricted to runners. The new location is too small to accommodate a major concert. "The real estate is just not available," said Mr. Furlow. "We don't want to run into overcrowding and congestion." An opening act will instead kick off the concert in tandem with the start of the 5K on Saturday night, followed by the Goo Goo Dolls' performance. The concert is free and open to the public, but there will be a security perimeter around the festival grounds. And behind the scenes, organizers will conduct surveillance and operate a central command station with its own medical team and law enforcement agencies.
Return to Top	

HEADLINE	**11/06 San Diego hepatitis outbreak grows**
SOURCE	**http://www.sandiegouniontribune.com/news/hepatitis-crisis/sd-me-hepatitis-numbers-20171106-story.html**
GIST	Though the case count in San Diego's ongoing hepatitis A outbreak increased again Monday, officials said that the number of new infections continues to slow. In a presentation to the San Diego County Board of Supervisors, Dr. Wilma Wooten, the county's public health officer, showed a chart that indicated there were 31 cases in October, significantly fewer than the 81 reported in September and 94 in August which saw the largest total of the outbreak so far. After seeing the chart, board chair Dianne Jacob had a to-the-point question. "Is it getting better, the same or worse?" Jacob asked. "We feel it's getting better," Wooten replied. The latest update bumped the outbreak's case total to 544, eight more than the 536 reported last week. The number of deaths did not increase, remaining at 20 after one new death was reported last week.

	Though the county has been providing weekly case, death and hospitalization updates, there has been some confusion, even among the Board of Supervisors, about what those numbers really mean. Supervisor Ron Roberts noted that the weekly escalation in cases in deaths gives the public the feeling that, every time a tally grows, that means the outbreak has grown. But that's not the case. Because new numbers are not added to outbreak totals until they've been confirmed by genetic testing that can take weeks to perform, the weekly numbers are not a perfect barometer of the outbreak's current severity. Roberts directed officials with the county Health and Human Services Agency to find a way to give the public a better sense of how many cases have occurred since the last update. "It seems to me we can give a much clearer picture by organizing our material a little better so that people like me can understand this and get a better feel for what's happening," Roberts said. Wooten said during her presentation Monday, as she and other local officials have said in recent weeks, that the number of new cases reported to her department on a day-to-day basis has continued to decline. "The number of cases that are being reported daily now has recently decreased to one or two a day compared to three or more a day," Wooten said.
Return to Top	

HEADLINE	**11/07 Church security scrutinized after massacre**
SOURCE	**https://ca.news.yahoo.com/fear-faith-church-security-scrutinized-texas-massacre-120546736.html**
GIST	SUTHERLAND SPRINGS, Texas (Reuters) - After one of the nation's deadliest mass shootings unfolded on their doorstep, pastors and parishioners around the tiny Texas hamlet of Sutherland Springs have begun asking whether guns have a rightful place inside their houses of worship. It is a debate that is echoing across the United States as security experts and some politicians ask churches to consider a wide range of enhanced measures to thwart tragedies like Sunday's deadly rampage at the First Baptist Church. Barbara Burdette, who knew the 26 people killed in the massacre and as well as the 20 wounded, is ready to see her church hire armed security, or allow congregants to carry their own concealed firearms for self-defense. "God is our protector," said Burdette, 62, "but I do still think that we need to have people with conceal carry." Her pastor at the First Baptist Church of La Vernia, a one-story brick sanctuary 7 miles from the shooting scene, said the issue of guns in church requires a delicate balance between providing safety instead of fear. Arming parishioners is not the only option. At the historic black church in Charleston, South Carolina, where a white gunman killed nine at a June 2015 bible study session, uniformed police officers now attend regular worship services. "It's part of our new normal," said Reverend Eric Manning at Emanuel African Methodist Episcopal Church, by phone. He said the church also created in-house security, as have most black churches in the region. Muslim and Jewish institutions for years have added security measures to address the threat of violence and hate crimes. The Council on American-Islamic Relations (CAIR) stresses the importance of security

	cameras, strong doors and clearing brush away from buildings so attackers have no place to hide. A law enforcement vehicle prominently parked in front of a house of worship is also a strong deterrent to crime, said Claude Pichard, director of Training Force USA, which worked with churches across the country to improve security after the Charleston shooting. The question of enabling, or even encouraging, parishioners to shoot back is a discussion particularly important to communities where guns are a part of life, such as rural Texas. In Sutherland Springs, the shooter was confronted as he left the church by a resident who shot and wounded him. Texas Attorney General Ken Paxton told Fox News that churches should consider whether they wanted parishioners to be armed as a way of preventing another tragedy. His state allows for the concealed carrying of handguns by licensed owners. It is not clear exactly how First Baptist Church, where the shooting occurred, addressed gun issues. A sheriff in Williamson County, Texas, a two-hour drive from the massacre, expects to discuss arming parishioners at a church security summit he is organizing in the wake of the attack. He said churches have a responsibility to ensure that responding officers can distinguish a protector from the assailant. "What are you doing to make sure we don't have a friendly on friendly fire?" said Sheriff Robert Chody by phone. New Life Church, a congregation of 10,000 people in Colorado Springs, Colorado, requires churchgoers to leave their guns in their vehicles, a decade after it was the scene of a deadly shooting that killed two. A parishioner trained in church security used a firearm to wound the shooter, preventing greater carnage, said pastor Brady Boyd. "Pastors are now waking up to this reality that we are not living in Mayberry anymore," he said, referring to the fictitious North Carolina hometown on the "Andy Griffith Show," a long-running 1960s television comedy. He pointed out that no church could have security in place to withstand an attack by a military-trained shooter using an assault rifle, the scenario that unfolded this weekend in Texas. About 10 miles from the shooting, Floresville Christian Fellowship Pastor Bennie Herrera said he needed to re-examine security but knows there is only so much that can be done. "We will not be gripped by fear," he said. "Faith will rise up and we will come together," he said.
Return to Top	

HEADLINE	**11/07 Puerto Rico needs 'unprecedented' help**
SOURCE	**http://abcnews.go.com/Politics/wireStory/official-puerto-rico-unprecedented-us-50986407?cid=clicksource_4380645_1_hero_headlines_headlines_hed**
GIST	Puerto Rico has suffered such extensive devastation from Hurricane Maria that its recovery will fail unless the island gets more U.S. help. That's the word from Natalie Jaresko, executive director of a federal control board that oversees Puerto Rico's finances. Jaresko tells Congress that the U.S. territory needs emergency and restoration funds "on an unprecedented scale" to restore housing, water and electric power.

	Puerto Rican authorities have estimated the island suffered $45 billion to $95 billion in damage in the September storm. So far, Congress has approved nearly $5 billion in aid. The head of Puerto Rico's power authority isn't testifying as scheduled before a House committee — citing "urgent efforts" on power restoration.
Return to Top	

HEADLINE	**11/07 New CPR guidelines for dispatchers, kids**
SOURCE	**http://q13fox.com/2017/11/07/healthy-living-new-cpr-guidelines-for-9-1-1-dispatchers-and-kids/**
GIST	The AHA says more people will survive cardiac arrest if emergency dispatchers give hands-only CPR instructions over the phone and if children receive rescue breaths in addition to chest compressions." The changes re-emphasize the importance of bystanders starting immediate chest compressions if they see an adult or child collapse in a suspected cardiac arrest. Immediate bystander help has been shown to double or triple survival chances among the more than 350,000 Americans who suffer out-of-hospital cardiac arrest each year. The AHA is recommending dispatch-assisted compression-only CPR instructions when cardiac arrest is suspected. It says telephone CPR not only assists the untrained caller, but it reminds the CPR-trained caller how to provide high-quality CPR in a stressful situation. Currently, only half of the nation's dispatchers provide telephone CPR, which has been identified as a critical intervention in the chain of survival for out-of-hospital cardiac arrest. The guidelines also support the need for compressions and rescue breaths during CPR for people younger than 18. More than 7,000 children die from an out-of-hospital cardiac arrest annually. In most cases, it is the result of a lack of oxygen, and rescue breaths can keep oxygenated blood flowing through the system. Bystanders play a key role in saving lives. The AHA says if you don't know CPR, learn it. Here are the guidelines for hands-only CPR from the AHA: **Hands-Only CPR Can Save Lives**. Most people who experience cardiac arrest at home, work or in a public location die because they don't receive immediate CPR from someone on the scene. As a bystander, don't be afraid. Your actions can only help. When calling 911, you will be asked for your location. Be specific, especially if you're calling from a mobile phone as that is not associated with a fixed address. Answering the dispatcher's questions will not delay the arrival of help. **How to Give Hands-Only CPR**. If you see a teen or adult suddenly collapse, call 911 and push hard and fast in the center of the chest to the beat of any tune that is 100 to 120 beats per minute. Immediate CPR can double or even triple a person's chance of survival.
Return to Top	*Here's a link to with more details on the new CPR guidelines:* *https://eccguidelines.heart.org/index.php/circulation/cpr-ecc-guidelines-2/*

HEADLINE	**11/07 More snow coming to Cascades**
SOURCE	**http://www.seattlepi.com/local/weather/article/Ski-snowboard-Seattle-winter-snow-sports-12339288.php**
GIST	Winter is in the air in Seattle, and even if the city isn't on track to flirt with any more snow soon, the mountains nearby are likely to collect at least a few inches this week. Those few inches could be enough to get one or two nearby ski areas open for the weekend.

	A weather system will start moving inland early Wednesday, bringing rain over lowland areas and snow to higher elevations, according to forecasts from the National Weather Service. While Snoqualmie Pass is expected to get a only few inches Wednesday and Thursday, farther south at Crystal Mountain, the NWS forecast is calling for anywhere from 15 to 27 inches. Crystal Mountain Resort indicated in a Monday update that, if the storm system delivers as promised, the resort plans to open Friday. To the northeast, Stevens Pass is expected to see possibly as much as 13 inches through Friday, an amount that might fall short of getting the ski area open but would be enough to have "something" happening at the resort this weekend, said Chris Danforth, vice president of sales and marketing for Stevens Pass Ski Area. "We're really just waiting to see what this next set of weather brings in," Danforth said Tuesday afternoon. "If we get another 15 inches of snow, we're probably opening." But Danforth left a big question mark on that "if," as a change in the forecast could shift that snow to rain in a hurry. Mount Baker Ski Area also is forecast to see upwards of two dozen inches of snow fall this week, but the area hasn't made any suggestion that an opening could come this weekend. With about 25 inches of pre-season snow at Heather Meadows, the area is "one or two good storms away from opening," according to the latest snow report. Baker typically opens between Nov. 19 and 22, and it's not unusual to get a last-minute announcement about an early opening. Back in Seattle, grab your Gore-Tex rain jacket and don't plan on leaving it at home any time soon. Rain is in the forecast into next week, and a cold front will come from the north Tuesday, bringing snow levels down to 3,000 feet and likely making for more heavy snowfall in the mountains next week, according to the NWS forecast discussion.
Return to Top	

HEADLINE	**11/07 King Co. voters approve more taxes**
SOURCE	**https://www.seattletimes.com/seattle-news/politics/king-county-proposition-1-veterans-homeless-seniors-2017/**
GIST	King County voters again approved a levy to fund services for veterans, the homeless and seniors Tuesday night, with 66 percent approval for the measure. The levy will raise roughly $354 million over the next six years, double the size of the previous veterans and human services levies approved in 2005 and again in 2011. In that time, the levy has become a flexible funding source to address the county's human-service needs, but this year, for the first time, King County officials decided to add spending on seniors to the funding package. The last tax measure on the King County ballot — a sales tax to fund arts, cultural and science education — failed in the August primary. But there was no organized opposition to Proposition 1, and supporters campaigned on the increasing need for more affordable housing as the county continues to face a homelessness crisis and the region's home prices remain on the rise. "This is clearly the voters of King County recognizing our obligation to those who have served our country, to those who've built the community, to make sure those people can live here securely and with dignity," said King County Executive Dow Constantine, who also sailed to reelection Tuesday night.

	At 10 cents per $1,000 of assessed property value, the tax will add about $45 more per year for a $450,000 home, the median assessed value in 2017, according to the King County assessor. Median housing values have since spiked in the subsequent months, so it is likely property owners will pay more than originally estimated.
Return to Top	

HEADLINE	**11/08 NKorea officials: done listening**
SOURCE	**http://www.cnn.com/2017/11/08/asia/north-korea-trump-speech-analysis/index.html**
GIST	Pyongyang, North Korea (CNN)North Korean officials were closely watching US President Donald Trump when he addressed the South Korean National Assembly Wednesday, but they say they weren't listening. Though the American leader's tone was more subdued -- and he proposed what some perceived as a conditional olive branch -- officials in Pyongyang authorized to speak for the government told CNN when it comes to Trump, "we don't care about what that mad dog may utter because we've already heard enough." Pyongyang accuses Trump and the United States of heightening tensions to a level not seen since the Korean War ended in an armistice in 1953. They say it's actions not words that matter, pointing to three US aircraft carriers and a submarine currently off the coast of the Korean Peninsula. "The United States is threatening us with nuclear aircraft carriers and strategic bombers. They are challenging us with with the most vicious and demeaning provocations but we will counter those threats by bolstering the power of justice in order to take out the root cause of aggression and war," the officials said. Trump did hint at a chance of diplomacy to resolve the standoff, but only if North Korea were to stop its provocative behavior, quit developing ballistic missiles, and agree to "complete, verifiable, and total" denuclearization. Most Korea-watchers believe that last item is a non-starter.
Return to Top	

HEADLINE	**11/07 King Co. sheriff trails in reelection race**
SOURCE	**http://www.king5.com/news/politics/king-county-sheriff-election/489641670**
GIST	Early returns show current King County Sheriff John Urquhart trailing challenger Mitzi Johanknecht. As of 8 p.m. Tuesday, Johanknecht held 52% of the vote while Urquhart had 48%. Urquhart, a 41-year law enforcement veteran, is wrapping up his first term as King County Sheriff. He served for several years previously as the office's public information officer. Johanknecht has spent 32 years in law enforcement and is a major in the sheriff's office commanding the southwest precinct. Johanknecht campaigned for Urquhart in 2013 but says she did not see the transparency in the department that was promised.
Return to Top	

HEADLINE	**11/07 Claim: Red Cross floundered Harvey relief**
SOURCE	**https://www.usatoday.com/story/news/nation-now/2017/11/07/red-cross-floundered-hurricane-harvey-relief-effort-texas-leaders-residents-say/839619001/**
GIST	For the American Red Cross, Hurricane Harvey presented a perfect chance at redemption.

A fast and efficient response would have shown critics the organization has learned from its past mistakes and is a capable partner when disaster strikes. But instead, say many Texas officials and residents, the Red Cross floundered and failed to provide needed help.

Weeks after the storm, state and local officials, including Gov. Greg Abbott, complain of a charity disorganized and slow-to-respond. The Red Cross' leader in the region hardest hit has resigned, complaining of a constant struggle to juggle the wants of the national office versus the needs of hurricane survivors. And many of those survivors have a long list of complaints.

The post-Harvey rancor has left the group synonymous with volunteerism and selflessness again on its heels, forced to reconcile negative reports on the ground with its reputation as the go-to during America's worst moments.

Aubrey Dominguez returned to find his Rockport home completely gone, but was denied Red Cross assistance. "They are good at driving around giving out hot meals," he said. "Other than that, that's about it."

One Texas lawmaker who represents a section of rain-pummeled Houston, where thousands of people lost their homes and belongings to Harvey's floods, said he's had enough with the missteps and confusion.

"I just won't give the Red Cross any more money," said state Rep. Garnet Coleman, a Democrat who has served 26 years in the Texas House. "I'll find other ways to help people in need."

In recent years, the Red Cross' reputation has taken repeated hits, spearheaded by reporting from NPR and ProPublica that highlighted lapses in how the organization spends its money and directs its resources. Then, a Congressional inquiry found the organization was using about a quarter of the money directed to the 2010 Haiti earthquake for other expenses. It also faces dwindling revenues, a smaller workforce and fewer volunteers than it did just a few years ago.

This round of criticism comes as the organization juggles a number of major disasters, from the hurricane trio of Harvey, Irma and Maria, to California wildfires and the mass shooting in Las Vegas.

As for Harvey, the Red Cross described its response as "massive," one that fulfilled its mission considering the historic nature of the storm, which dropped more than 50 inches of rain.

"In a disaster, you don't get everything perfect every time," said spokeswoman Elizabeth Penniman, "but the incredible number of people we sheltered and meals we served and comfort and care we provided prove we fulfilled our mission, and some of the criticism does not take into account the size and scale of our response."

Bob Ottenhoff, the CEO and president of the Center for Disaster Philanthropy, said the Harvey response proved to be a huge challenge for relief organizations, but called it overall "pretty good." Still, it's not over.

"The challenge confronting us now and the thing that often proves to be very frustrating to homeowners and business owners, is the fact that the recovery period is so complicated and so long," he said. "There's a tremendous amount of work before us that is going to be very difficult."

Much of his criticism centers on the Red Cross' dispersal of funds and the fact that he said it took a couple weeks into the recovery process "before they even set up shop."

As a first step in recovery plans, the Red Cross offered $400 funding payments meant to address immediate needs, like clothing and food, for disaster survivors. Some applications were thought to be mistakenly rejected due to technological issues. Penniman said the initial demand "challenged our IT infrastructure," leading to a temporary suspension in service.

The Red Cross' focus during a disaster is on shelter, food and emergency relief supplies, among other duties. Its 270 chapters provide the immediate response while operating off a “clear framework” which provides chapters the flexibility to meet local needs while “maintaining consistent services to support our mission,” Penniman said.

When a situation requires a national-level response, such as in Harvey, oversight shifts to Red Cross headquarters in Washington, D.C.

David Brady, the ex-CEO of the Red Cross’ Texas Gulf Coast region, which serves places like Houston, Galveston and Corpus Christi, found such an arrangement to be a struggle. After he resigned, he spilled his feelings on Facebook.

“My challenge was a daily struggle to do what is best and serve the national organization that pays my salary and doing what is best and serving my fellow Texans and this community I love so much,” the Facebook post said, according to KHOU-TV in Houston. “I found myself in disagreement too often with decisions that were being made as it related to Hurricane Harvey recovery.”

In recent years, the Red Cross has watched its resources shrink.

From 2008 to 2016, tax records show the organization saw a 41% percent dip in employees, and revenue fell by nearly $700 million to about $2.6 billion as volunteers more than halved from about 662,000 to 314,000.

That goes against the current trend, Ottenhoff said. Relief organizations are seeing more and more volunteers.

Donations nowadays are more directed to local relief organizations rather than large ones, said Charity Navigator spokeswoman Sara Nason. The website, which evaluates charities and facilitates donations during disasters, directed about $3.1 million in the 17 days after Harvey to organizations supporting the relief effort. The majority went to small organizations in Texas.

"A lot of individuals we saw were looking to donate specifically to local organizations because they saw the value of this long-term commitment to the area," she said.

Penniman seemed to dismiss any notion that the lower numbers have affected the charity’s response. The Red Cross operates in 90% of America’s counties, she said, and has grown more efficient and effective through technology.

Roughly 9,500 Red Cross disaster workers assisted with Harvey — 110 are still there — and the organization raised $429 million, more than was raised during Hurricane Sandy. Its financial assistance program has provided $400 payments to 573,000 people, equal to $229 million. That leaves about $200 million in the coffers. An estimated budget of its Harvey expenses at the end of September showed 91% of the funds will go to programs and expenses.

“We have spent more money on more people in a shorter time period than any disaster response since Hurricane Katrina,” Penniman said.

Ottenhoff said government and nonprofits are better organized and more sophisticated at disaster response than they were 10 or 20 years ago, partly because of lessons learned after Hurricanes Andrew and Katrina. The Red Cross, Penniman said, is a “learning organization” that’s always looking to improve.

In the meantime, frustration remains.

“They have such a bad reputation in this community that it would be better for them not to come back,” said Bujan, the Port Aransas mayor.

Return to

Top

HEADLINE	**11/08 Protesters disrupt transportation Catalonia**
SOURCE	**http://abcnews.go.com/International/wireStory/striking-protesters-disrupt-transportation-catalonia-51007949?**
GIST	Protesters have blocked roads and stopped commuter trains as Catalonia faces a general strike in the wake of unprecedented controls in the region by Spanish central authorities to crush an independence bid. Intersindical CSC, a platform that groups pro-independence workers' unions, had called the strike for Wednesday to push for labor rights. But the call comes at a sensitive political moment, and separatist parties and civil society groups asked workers to join the stoppage to protest the jailing of activists and ousted Catalan government officials. Spanish authorities took direct control of Catalonia after regional lawmakers passed an independence declaration on Oct. 27. An early election has been called for next month to replace the sacked regional government. Among dozens of roads blocked, protesters cut the traffic on the AP7 motorway north of Girona, one of the main arteries connecting France and Spain.
Return to Top	

HEADLINE	**11/08 Philippines backs down in S. China Sea**
SOURCE	**http://abcnews.go.com/International/wireStory/philippines-backs-china-sea-beijing-protest-51003699**
GIST	Philippine President Rodrigo Duterte stopped construction work on a newly formed sandbar in the disputed South China Sea after China protested, the defense chief said Wednesday, disclosing details of the territorial spat for the first time. The dispute over a string of sandbars called Sandy Cay emerged in August and prompted China and the Philippines to consider negotiating some sort of arrangement to prevent such incidents from spiraling out of control, Lorenzana said. The rift over the tiny sandbar, where Filipinos planned to erect fishermen's shelters, in the group near Philippine-occupied Thitu island in the Spratlys archipelago remains unresolved but both sides pledged not to occupy any new territory, he said. China's claims to most of the South China Sea overlap those of the Philippines and four other governments. Despite that, tensions have eased since Duterte took over as president last year and took steps to thaw once-frosty relations with Beijing. Duterte has courted Chinese trade and assistance and taken a nonconfrontational approach to their territorial disputes. He has refused to immediately take up with China a ruling by a U.N.-linked tribunal that invalidated Beijing's sprawling claims in the South China Sea, sparking criticism from nationalists and left-wing groups, which wanted him to demand immediate Chinese compliance with the landmark decision. "We tried to put some structures in one of the sandbars near our island and the Chinese reacted," Lorenzana told a diplomatic and security forum in Manila, adding that Duterte later ordered, "Let's pull out."
Return to Top	

HEADLINE	11/08 India lauds last year's rupee swap
SOURCE	http://abcnews.go.com/International/wireStory/india-lauds-years-rupee-swap-economy-slows-51008733?
GIST	One year after India overhauled its currency, yanking 86 percent of its notes out of circulation without warning, many Indians still aren't sure if it was worth it. Economic growth has slowed. Unemployment has risen. And corruption remains a scourge nationwide. Prime Minister Narendra Modi's government insists the move to replace most of the country's currency has been a success, and declared Wednesday as "Anti-black money day" to celebrate the country's fight against money laundering and tax evasion. But former Prime Minister Manmohan Singh of the opposition Congress party called the move "reckless" and said that, while India needed to tackle tax evasion and fraud, "demonetization was clearly not the solution."
Return to Top	

HEADLINE	11/07 Uncle in Kelso messaged Texas shooter
SOURCE	http://komonews.com/news/local/texas-gunmans-uncle-messaged-him-from-wash-state-before-shooting
GIST	PORTLAND, Ore. - The uncle of the man that authorities say opened fire in a Texas church Sunday, killing 26 people, is a resident of Kelso, Wash., and says his nephew acted as a "coward." On Monday, Dave Ivey spoke with the hosts of Northwest Digital News and said he reached out to his nephew, Devin Patrick Kelley, just hours before the shooting in Sutherland Springs, Texas, on Sunday. "He posted on Facebook that he wasn't thinking correctly. His head hurt. So I private messaged him, and I said, 'Hey Devin, what's up? Are you OK, bud? Have a shot of whiskey or something. Life is good. And I didn't get a response from him, and then this happened," Ivey said. "My personal opinion at this point - my nephew, he acted as a coward. He took a lot of innocent life, and I'm sorry." Ivey said he last saw his nephew about 20 years ago, but they used social media to stay in touch. Ivey also said he wants to raise money for the victims and their families. Authorities believe Kelley died of a self-inflicted gunshot wound.
Return to Top	

HEADLINE	11/07 Record 456tons unused pills collected
SOURCE	https://www.upi.com/Top_News/US/2017/11/07/Record-456-tons-of-unused-pills-collected-in-one-day/4781510081638/?utm_source=fp&utm_campaign=ts&utm_medium=3
GIST	Nov. 7 (UPI) -- Pharmacies and police stations nationwide collected a record 456 tons of expired, unused and unwanted prescription drugs in a specially designated day last month. During the 14th National Prescription Drug Take Back Day on Oct. 28, the 912,305 pounds were turned in to 5,300 affiliated collection sites, the Drug Enforcement Agency said in a release. The haul, which included heroin, opioids fentanyl and oxycodone and other prescription drugs, is almost six tons more than was collected at last spring's event.

	Since fall 2010, when the event began, DEA has collected 9,015,668 pounds, or 4,508 tons, of prescription drugs. "In the midst of the worst drug crisis in American history, drug abuse prevention has never been more important," Attorney General Jeff Sessions said in a statement. "And at the Department of Justice, it's what we do every day. By taking dangerous drugs off of our streets, we keep addiction from spreading. One of the most important ways we do that is through the DEA's semi-annual Prescription Drug Take Back Days." The DEA, which is part of the Department of Justice, set up 115 collection sites on tribal lands for the first time in the semiannual event. In all, there were 4,274 law enforcement partners. The state with the post drugs collected was California with 70,260 pounds -- followed by 67,273 in Texas, 60,257 in Wisconsin, 44,081 in Illinois, 42,850 in New York and 41,700 in Maine. "At a time like this, this event is having more of an impact than ever," Sessions said. "I want to thank all of our local law enforcement partners who helped at all 5,300 collection sites to make this possible-and everyone who participated. They're helping us end this crisis one pill at a time." The DEA's Drug Take Back website gives information on safely disposing of drugs, including locations. The next Prescription Drug Take Back Day is April 28.
Return to Top	

HEADLINE	**11/07 FBI raids HQ body broker firm**
SOURCE	**http://www.reuters.com/article/us-usa-bodies-fbi-exclusive/exclusive-fbi-agents-raid-headquarters-of-major-u-s-body-broker-idUSKBN1D72SL**
GIST	PORTLAND, Oregon (Reuters) - Federal agents have seized records from a national company that solicits thousands of Americans to donate their bodies to science each year, then profits by dissecting the parts and distributing them for use by researchers and educators. The search warrant executed by the Federal Bureau of Investigation at MedCure Inc headquarters here on November 1 is sealed, and the bureau and the company declined to comment on the nature of the FBI investigation. But people familiar with the matter said the inquiry concerns the manner in which MedCure distributes body parts acquired from its donors. MedCure is among the largest brokers of cadavers and body parts in the United States. From 2011 through 2015, documents obtained under public-record laws show, the company received more than 11,000 donated bodies and distributed more than 51,000 body parts to medical industry customers nationally. In a current brochure, the company says that 80,000 additional people have pledged to donate their bodies to MedCure when they die. FBI spokeswoman Beth Anne Steele confirmed the day-long search of the 25,000-square-foot facility, but declined to comment further because the matter is under seal. A person familiar with the matter said that FBI agents took records from MedCure but did not remove human remains. The search warrant, though sealed, signals that an FBI investigation of MedCure has reached an advanced stage. To obtain a search warrant to seize records, rather than demand them via subpoena, FBI agents must provide a detailed affidavit to a U.S. magistrate with evidence to support probable cause that crimes have been committed and that related records may be on the premises.
Return to Top	

HEADLINE	**11/07 Subsidized sex assault 'hush money'**
SOURCE	**https://www.cbsnews.com/news/taxpayers-subsidize-hush-money-for-sexual-harassment-and-assault/**
GIST	Many of the recent stories about sexual abuse claims against disgraced Hollywood mogul Harvey Weinstein, former Fox News host Bill O'Reilly and other powerful actors, journalists and executives mention settlements either they or their employers made to silence women who accused them of misconduct. These settlements often require alleged victims to sign a nondisclosure agreement – essentially a pledge of secrecy – in exchange for a cash payment. They are designed to keep the reputations of allegedly abusive high-flyers intact, an arrangement that can allow repeated wrongdoing. As a law professor who focuses on white-collar crime, what I find striking about these contracts is how they can be treated as tax-deductible business expenses. That means American taxpayers are helping foot the bill for keeping despicable behavior in the shadows. The payments associated with these settlements can be treated as a business expense. That means they are tax-deductible, as long as they are related to the conduct of the company's ordinary operations. Although it might seem odd to say that sexual harassment is within the realm of a company's business, the many accusations against Weinstein involved encounters that were at least purportedly related to future movie productions. Either an employer or the person accused of harassment can pay the money required by these settlements. In O'Reilly's case, Fox has said it knew that he had reached a new settlement with an accuser before it renegotiated his contract earlier this year. Fox's insistence that the company was unaware of the size of the settlement – $32 million – makes it clear that O'Reilly wrote the check. Even the attorney's fees for negotiating the settlement are deductible as another ordinary business expense. Until about 50 years ago, payments related to violations of what the courts deemed violations of "public policy" were not tax-deductible. Congress changed that in 1969. Section 162 of the U.S. tax code now only explicitly prohibits the deduction of bribe payments, health care kickbacks, lobbying expenditures and any fines or penalties paid to the government for violating the law. Just about everything else is deductible. But most victims of sexual harassment and abuse do not get a break. That's because the law exempts payments only for physical injuries, not for payments related to emotional distress.
Return to Top	

HEADLINE	**11/07 India air 'public health emergency'**
SOURCE	**http://abcnews.go.com/International/severe-air-pollution-declared-public-health-emergency-delhi/story?id=50987745**
GIST	The city of Delhi, India, is surrounded by a thickening blanket of smog that covers the city, making the sky less visible and the air less breathable. The Indian Medical Association (IMA) declared a public health emergency in the city on Tuesday -- the city's air quality rating is above the highest levels on the index. People have been advised to avoid any outdoors activity and to keep children indoors to avoid the risks of the "severely harmful" air quality. The Education Minister confirmed elementary schools will be closed on Wednesday, saying an extension of the order is possible. Delhi Chief Minister Arvind Kejriwal published statements on Twitter today, including a request to Sh. Manish Sisodia, Deputy Chief Minister, to consider closing schools for a few days.

	The problem is expected to linger for some time. The Doctors Association's requested that Kejriwal cancel the Airtel Delhi Half Marathon, according to local media reports, which is about two weeks from now, on November 19. Flight schedules have also been changed due to low visibility today; more than 20 flights have been delayed and at least four have been rerouted. The Air Quality Index (AQI) in Delhi is currently 316, which is above the threshold for "severely polluted" and has health implications, according to officials. The AQI scores range from excellent and good at 0- 50 and 51-100, lightly polluted and moderately polluted at 101-150 and 151-200 and heavily and severely polluted are 201-300 and 300-plus.
Return to Top	

HEADLINE	**11/07 Baltimore cop cleared in Gray case**
SOURCE	**http://abcnews.go.com/US/wireStory/panel-disclose-verdict-police-van-driver-case-50985617**
GIST	A disciplinary panel has found a Baltimore police van driver not guilty on all administrative charges related to his transportation of Freddie Gray, the black man whose death in custody sparked riots in the city. The three-member board said Tuesday that Officer Caesar Goodson did not violate any department policies the day Gray was fatally injured in police custody. Goodson smiled, appearing relieved, after the not-guilty verdicts on all 21 counts were read. His lawyers hugged each other and patted themselves on the back with loud thumps. Attorney Sean Malone said outside the hearing room at the University of Baltimore that the verdict is vindication for a hard-working and soft-spoken officer. He also said that Goodson plans to keep working on the Baltimore police force. Department lawyer Neil Duke had argued that Goodson should have been fired for failing to follow policy by not buckling Gray into a seatbelt, failing to get him medical attention and lying about the chain of events following Gray's arrest in April 2015. Gray died a week later of a spinal cord injury he suffered during the van ride, prompting civil unrest among people expressing outrage at the treatment of African-Americans by police in Baltimore's inner city. None of the six officers charged criminally for their roles in Gray's arrest were convicted. In reforms made as a result of Gray's death, state lawmakers opened police disciplinary hearings to the public, hoping to improve transparency when departments seek to hold officers accountable.
Return to Top	

Cyber Awareness

Top of page

HEADLINE	**11/07 Growing threat synthetic identity fraud**
SOURCE	**https://dealbreaker.com/2017/11/recent-federal-indictments-highlight-the-growing-threat-of-synthetic-identity-fraud/**
GIST	The unsealing of four federal indictments last April, which charged 19 suspects with a range of fraud and money-laundering offenses, revealed glaring holes in banks' identity management practices. These charges are the result of a six-year, multiagency investigation led by the Federal Bureau of Investigation (FBI), which revealed a transnational conspiracy that orchestrated the theft of more than $13 million from 170 victims, primarily based in the United States.

The conspiracy crossed the borders of Europe, Israel, and the United States, and involved four interconnected criminal schemes: online vehicle fraud, business email compromise (BEC), unlicensed money transmitting, and international money laundering. To date, authorities have brought 17 suspects into custody and are actively searching abroad for the other two, who remain at large.

At the press conference where the U.S. Attorney's Office for the District of Columbia revealed the charges, federal prosecutor Channing Phillips said the "investigation uncovered an interconnected web of money launderers and fraudsters and individuals who enabled their criminal activity."

Despite being unwilling counterparties, some 45 American banks also enabled this criminal conspiracy to flourish with their porous customer identification programs (CIP) and Know Your Customer (KYC) processes. Specifically, the online vehicle & boat fraud ring, which underpinned the entire investigation and functioned as the "gateway" scheme, relied on synthetic identity fraud (SIF) – a method that has grown increasingly popular in the global underworld. Last year, The Wall Street Journal identified SIF as one of the top three risk issues facing the banking industry. In SIF schemes, criminals use partially or entirely falsified consumer data to open new accounts (New Account Fraud or NAF), procure credit cards, or apply for loans.

The Csurgo identity

According to FBI documents, the online vehicle con worked like this: fraudsters from Europe would place false online advertisements for cars and boats on e-commerce platforms such as Ebay and Cars.com; deceived buyers would wire funds to the U.S. or an international bank account specified by the seller; and fraud coconspirators would immediately withdraw the money, launder it, and send theft proceeds back to their associates in Europe before the banks and victims detected the scheme. The only reason the conspiracy worked is that the perpetrators withdrawing the stolen funds had used counterfeit identification documents to open dummy bank accounts, making them invisible to investigators.

Specifically, the U.S.-facing component of the fraud depended on Hungarian national Istvan Csurgo using fictitious driver's licenses and passports, provided by his foreign accomplices, to open accounts at over 40 banks in the District of Columbia, Maryland, New Jersey, New York, Pennsylvania, and Virginia. In 2012, Csurgo pled guilty to one count of conspiracy to commit bank fraud and one count of use of a false passport. He also admitted to authorities that he stole or attempted to steal approximately $756,511 from fraud victims, while his coconspirators netted roughly $1 million from the scheme.

The synthetic ID fraud paradigm shift

The Csurgo case is emblematic of bank fraud's paradigm shift away from customer impersonation to synthetic ID generation and NAF, the latter of which more than doubled in 2015, compromising 1.5 million consumers – up from 700,000 in 2014. This underworld trend is the result of widespread EMV (Europay, Mastercard, and Visa) chip credit card adoption in the U.S., which makes it harder to counterfeit consumer credit cards and has pressured criminals to alter their strategy. Also, the spike in online consumer data theft, which has spawned a market for stolen ID credentials on the Dark Web, an encrypted network that is inaccessible to traditional search engines, has created an optimal evolutionary ecosystem for SIF perpetrators.

The anonymity offered by the Dark Web has not gone unnoticed by traditional organized crime groups (OCGs), which have co-opted and criminally optimized SIF rings, inculcating them with generations of deviant expertise. Alternately, fraudsters are also forming their own coordinated criminal networks of hackers and money mules to rob financial institutions (FIs) and consumers. According to Richard Parry, a consultant and a former security executive at JPMorgan Chase, Citigroup, and Visa, a typical SIF ring has hundreds and sometimes thousands of fake IDs going at the same time. In 2014, technology research firm Gartner estimated that SIF schemes account for 20 percent of credit charge-offs, where creditors determine that a debt is unlikely to be paid, and 80 percent of all credit card fraud losses.

	A culture of silence Total SIF losses to banks remain unknown because FIs prefer not to publicize this data. Typically, investor relations and reputation-management considerations create an incident-response culture, where "there's no self-reporting victim," according to Parry. In fact, banks usually fail to detect synthetic accounts and incorrectly classify fraud as loan losses. But, to articulate the scope of the problem, consider that in 2013, authorities exposed an organized SIF ring based in New Jersey that created 7,000 fake IDs to obtain more than 25,000 credit cards, enabling the theft of over $200 million from issuers. Common SIF tactics Criminals generally create synthetic identities in one of the following three ways: • Pair a real Social Security number (SSN) with a fake name • Use an "inactive" SSN with a real name (typically belonging to a child or someone who has died) to pass KYC filters • Fabricate both the SSN and the name completely Further, the Social Security Administration's move away from an "orderly, rules-based numbering scheme" to random number generation in 2011 has allowed more numbers to be created, thus making it harder for institutions to distinguish legitimate SSNs from fake ones. According to Garient Evans, Vice President of Solution Services at ID Analytics, SIF rings will generate SSNs that are one digit off or change the sequence of numbers. "They'll do things such that an actual credit bureau file will be pulled, because the Social Security number is close enough and a lot of institutions have fuzzy logic," he told American Banker. Further, Sonya Andreassen-Henderson, vice president of the mortgage investigative services group at PNC Bank, told The Wall Street Journal that criminals will also leverage fake pay stubs, fictitious businesses, and fabricated references to fraudulently obtain legitimate banking services.
Return to Top	

HEADLINE	**11/07 Hackers exploit New York terror attacks**
SOURCE	**http://thehill.com/policy/cybersecurity/359221-fancy-bear-capitalizes-on-new-york-terror-attacks-to-lure-new-victims**
GIST	The Russian government-affiliated hacking group Fancy Bear took advantage of the New York terror attacks on Halloween to lure new victims, according to a new report from McAfee. The attack affixes a command to download malware to a word document about the attacks titled "IsisAttackInNewYork.docx." In late October, Fancy Bear used a similar tactic to hack people interested in military cyber security, using a document that appeared to contain information about the CyCon cybersecurity conference sponsored by West Point, currently ongoing in Washington, D.C. That attack was first identified by Cisco's Talos labs. "Based on the telemetry we captured, we have observed targets in Europe, specifically France and Germany," said Ryan Sherstobitoff, senior analyst for major campaigns for McAfee Advanced Threat Research via email. "Based on the document theme from the previous related campaign, it has a name SabreGuardian, which is in reference to the U.S. Army in Europe" Fancy Bear is best known as one of the Russian hacker groups believed to have hacked the Democratic National Committee during the 2016 election.

	The new attacks differ slightly from the CyCon attacks. The CyCon document used a feature in Microsoft Word known as a VBA script to download the Seduploader malware. The New York attack document takes advantage of a different feature, known as Microsoft Office Dynamic Data Exchange, to download Seduploader. Dynamic Data Exchange is intended to share data between documents. McAfee believes that the change in tactic may have come due to the surprisingly widespread attention garnered by the CyCon attack, which may have caused users to adapt.
Return to Top	

HEADLINE	**11/07 Report: DHS cyber intel sharing falls short**
SOURCE	**https://www.cyberscoop.com/house-committee-report-fusion-centers-dhs-cyber-nccic-nppd/**
GIST	Fewer than one-in-four Homeland Security fusion centers across the country receive cyberthreat reporting or other intelligence products from DHS' National Protection and Programs Directorate, hampering their nascent efforts to help defend the country against online attacks, a congressional report said Tuesday. Those efforts are further hampered because fusion center representatives do not sit on the floor of NPPD's 24 hour watch center, the National Cybersecurity and Communications Integration Center (NCCIC), the majority staff of the House Homeland Security Committee found. The report includes material from dozens of interviews and a long survey completed by 68 major fusion centers across the country. The centers were set up to integrate state and local law enforcement agencies into DHS' homeland protection mission by providing them with threat warnings they could use to inform their local priorities and by vacuuming up local intelligence reporting in the hope that it could cast light on national trends or geographically dispersed terrorist plotting. "Significantly, only 16 out of 68 survey respondents reported they receive NPPD cyber-related products," reads the report, "Given current cyber threats and fusion centers' nascent efforts to develop cybersecurity capabilities, the committee believes DHS should ensure these products are made accessible to fusion center personnel, when appropriate." One problem with the NPPD intelligence: It's too highly classified. "A significant amount of cyberthreat information is classified at the Top Secret level, which has prevented some fusion centers from conducting analysis on this issue" because they lack the special facilities required to receive and store top secret information, states the report. Even the half of all fusion centers which do have a special room, known as a SCIF, to receive and store classified reporting, cannot share it with the state and local law enforcement agencies they're supposed to work with due to a lack of clearances for state-level employees. "Their ability to share it with their state and local partners is restricted because there are a limited number of products at the Sensitive but Unclassified (SBU) level," reads the report. DHS leadership "should proactively work with the NCCIC to develop a process for sharing cyber threat information with fusion centers at the unclassified level," the report recommends.
Return to Top	

HEADLINE	**11/07 Expert: cyber threat to UK railways real**
SOURCE	**http://www.railtechnologymagazine.com/Rail-News/cyber-security-vital-after-four-attacks-on-britains-rail-network-last-year**

GIST	Digital technology must play a part in improving organisational resilience and reducing passenger safety risk, a leading rail industry figure has stated. Speaking at Rail Network Resilience 2017 last week, Arup's resilience, security and risk associate, Nadim Choudhary, said that cyber security is a very real threat to Britain's railways. The cyber security threat is so great that the government has added it to its tier 1 threats, alongside terrorism, war and global pandemic. Every 4.7 seconds there is a new malware threat introduced to the internet. In the past, security threats were physical systems with no online connectivity, however, in the last year alone there have been four major cyber-attacks on the railways. Previously the development of operational technology (OT) and information technology (IT) have been treated as separate entities, but Choudhary said that this is changing. The railways are joining the 21st century and the two systems are merging, which exposes the network to more cyber-attacks. In response to this, safety is now becoming embedded in the IT systems of the railways, but this is not without its challenges. However, this impacts on business continuity and, if it becomes a frequent event, it will undermine the public's confidence in the network, as well as having a financial impact on companies due to imposed fines for failure to meet the agreed service. Choudhary explained that natural events expose the industry to cyber threats: "If we have a natural hazard event, or we have a flooding event, or whatever event we have, cyber criminals are very resourceful - they know when systems are down and they will attack things when organisations are at their most vulnerable." The industry needs to have a joined up approach to developing a coherent strategy for maintaining cyber security, identifying gaps for research, and standards and guidance need to be issued, he advised. The supply chain also needs to be robust and resilient, and collaboration with peers is vital to establish what the cyber risks are. "Cyber security should be considered a fundamental part of an organisation," he continued. "It shouldn't just be a bolt-on, added at the end, it should form part of the solution, it should be at the outset of the design when we are considering and designing our systems and components, and cyber security should be a part of that."
Return to Top	

HEADLINE	**11/07 Experts: threats to satellites are legion**
SOURCE	**http://spacenews.com/cyber-experts-say-threats-to-satellites-are-legion/**
GIST	WASHINGTON — If your company or organization uses a network, there are people who want to hack it. If you haven't tried to stop them, those hackers are probably already in your network. That was the message from cybersecurity experts at the CyberSat Summit here Nov. 7. Satellites are just another target in a cyber world rife with perpetrators. "It's not if, it's when," James Turga, executive assistant director of the FBI's Information and Technology Branch, said about getting hacked.

	Turga said around 1.4 million new phishing sites form every month, and ransomware sold on a hidden level of the internet known as the "dark web" has gone up 2,500 percent. "Those are staggering numbers and the amount of tools that are out there because of various leaks from organizations have now caused a situation where the threat is so prolific, [that] it doesn't matter if you are 'mom and pop' or a Fortune 500 company or the FBI or NASA." Lisa Donnan, managing director of Option3Ventures, a venture capital firm focused on information security and analytics companies, said conversations with chief security officers (CSOs) have shifted from defense to damage control given the magnitude of cyber attacks. "When the average breach has been there for 221 days — on average — the game's over," she said. "When you speak to seasoned CSOs, their mindset is much more in resiliency and recovery, because they've lost the war." Donnan said traffic running on satellite networks — defense communications, financial information and television broadcasts, for example — are all very attractive to hackers. Option3Ventures always considers what digital infrastructure companies are building their businesses on, she said, and isn't interested in those using outdated technologies. Greg Touhill, president of the data center company Cyxtera Technologies' Federal Group, disagreed that the war has been lost, but said there are a myriad of threats to satellite systems. "We need to have the approach that 'I might be able to live through a battle I've lost, but I don't want to lose the war.' You have to have resiliency. You have to be able to take a punch and keep on going," he said. Risks include distributed denial of service (DDOS) — cyber-attacks designed to overwhelm a system and render it inoperable — to interrupt satellites and even launches, he said. If a hacker gets into the design phase of a satellite, they could even do a "Death Star"-type attack, implanting a weakness for exploitation at a later date, he said. "We've got folks that don't necessarily have that mindset of thinking like a hacker," he said. "You can buy down your risk if you start thinking like a hacker and adjusting the training, the certification, the auditing of your personnel processes and technology." Randy Sabett, head of Cooley's cyber practice, said intentionally misleading emails containing malware are the source of many new attacks, particularly those requiring electronic signatures.
Return to Top	

HEADLINE	**11/07 Shipping faces expanding cyber threats**
SOURCE	**http://www.breakbulk.com/news-shipping-faces-evolving-expanding-cyber-threats/**
GIST	The threat to shipping and logistics from cyber attacks is "evolving and expanding" with the size of the current threat "underplayed due to a reluctance within the industry," according to international law firm Ince & Co. The firm called on operators to do more to prepare for attacks following a spate of incidents in the recent weeks. Greater digitalization, advances in satellite communications, and a drive towards greater technological efficiencies have all contributed to the increased risks according to Rory Macfarlane, cyber specialist at Ince & Co. "It is imperative that shipping companies act to mitigate their cyber-risk now, before they become the next victim of a major breach … Throughout 2017, we have seen headline-worthy cyber-attacks occur with growing frequency and severity. As new technologies emerge to streamline operations, cut costs and

	increase efficiencies, evolving and expanding cyber-threats also emerge," Macfarlane said. Ince & Co operates a network of affiliated commercial law firms with about 100 partners and more than 190 other lawyers advising clients throughout the global network.
Return to Top	

HEADLINE	**11/07 New technology cyber threats to aviation**
SOURCE	**https://www.ainonline.com/aviation-news/business-aviation/2017-11-07/report-new-technologies-raise-cyber-threat-aviation**
GIST	A group of security, defense and aerospace experts are releasing a report today to highlight the threats that exist to aviation cybersecurity and underscore the need for a clear vision to protect against those threats as technologies rapidly advance. The Washington think-tank Atlantic Council brought together airlines, airports, air traffic management specialists and other stakeholders to develop the report, Aviation Cybersecurity—Finding Lift, Minimizing Drag, which finds that preventive measures act as a deterrent, but "declarations of fully secure systems are unrealistic." Aviation systems in the past were relatively secure from cyber threats due to the "bespoke nature" of their design and their isolation from other systems, the report notes. "But air traffic management (ATM) is no longer isolated, and ground services and supply chains are becoming fully integrated into an interconnected digital world." The report points to vulnerabilities associated with emerging capabilities, ranging from additive manufacturing to unmanned systems, and warns that "their novelty may obscure the cybersecurity risks these technologies introduce." A shift from legacy radar to GPS and ADS-B greatly improve accuracy and reliability under normal conditions, the report states, but adds those systems "remain susceptible to degradation by environmental hazards or manipulations by hostile actors." Airports, which are susceptible to physical breach, are another area of concern, says the report, pointing to numerous other vulnerable areas, such as connectivity systems on aircraft, electronic flight bags and remote towers. Concerning to the report's authors is "the speed of innovation, technological advancement, and adversary capabilities potentially outstripping policy and regulatory development in many areas of the aviation ecosystem." The report offers numerous recommendations for shaping a cybersecurity vision, with a need to focus on international collaboration on managing risks and developing resilient systems. Recommendations range from reinforcing standardization, developing a common understanding of cyber safety and developing robust threat models, to designing systems to capture cybersecurity relevant data and training for safety. Another recommendation: "incorporate cyber perspectives into accident and incident investigations."
Return to Top	

HEADLINE	**11/07 Lessons from critical infrastructure**
SOURCE	**https://www.automationworld.com/article/technologies/security/cybersecurity-lessons-critical-infrastructure**
GIST	Though it's been almost two years, the cyber attack on the Ukrainian power grid in December 2015 still reverberates through the power plant community. The attackers took out a quarter of a million homes in the dead of winter, rendering them dark and cold just two days before Christmas. Operators were locked out of their own control systems, helpless to react as they watched the attack unfold on their screens, one system after another coming down. Attackers struck again using different methods a year later.

In response, operators and their vendors here in the U.S. and around the world wasted no time trying to secure their own plants. These actions and the best practices they are employing can also help manufactures in non-critical industries meet the growing threat from cyber attacks against increasingly connected systems.

Siemens, for example, has built a portfolio of operational technology (OT) network infrastructure for its own use, and is now rolling it out to its customers. “We call it First Line of Defense,” says Leo Simonovich, director of global cyber strategy at Siemens. These systems have OT security built in that follows the best practices outlined by others in the industry, including the North American Electric Reliability Corp. (NERC).

Attacks on the rise

The Ukrainian power grid is just one example of the rising number of critical facilities and industrial networks coming under attack across a wide range of industries. Many of these attacks are not specifically targeted at industrial networks, explains Galina Antova, CEO of OT security supplier Claroty. “The industrial networks have been affected by some of the ransomware attacks out there. They were not necessarily targeting the industrial networks, but ended up impacting the industrial networks nonetheless.”

WannaCry, a particularly virulent strain of ransomware—software that encrypts victims’ networks and holds them for ransom—caused widespread harm when it struck in May. Older networks—many of which are industrial networks—are particularly vulnerable to attack. Chocolate maker Mondelez International was one of several manufacturers reporting revenue lost to ransomware in 2017.

Part of what has made these attacks so effective is that cyber criminals now have access to more sophisticated tools than ever before, Antova says. “It's the first time in history that non-nation-state actors have access to nation-state capabilities,” she says. Following an August 2016 attack on the U.S. National Security Agency (NSA), hackers have distributed tools developed by the spy agency through the digital underground. “Now you've got the ultimate weapon; you've got a nation-state weapon.”

OT, controlling the machines running manufacturing processes, could be particularly vulnerable to cyber attacks. It is the new risk frontier, Simonovich says. “We've seen that those attacks are having big impacts on performance of plants with some pretty scary outcomes.”

Two factors combine to increase risk to OT, Simonovich says. To begin with, many industrial processes lack the readiness that is often more common in the business IT world. “Things like patching, configuration management—the basics, the hygiene,” he says. “The speed and the sophistication of the attacker has also increased.”

It’s no wonder, then, that a recent survey about cybersecurity in the oil and gas industry conducted by the Ponemon Institute and funded by Siemens found that 68 percent of respondents believe their organizations have been compromised by at least one cyber attack.

Fortunately, best practices can go a long way toward mitigating the risk.

Cybersecurity best practices

Cybersecurity for OT has to start at the top—someone in a senior leadership position has to be responsible for cybersecurity, Antova says. The most logical person for the job, she says, is the chief security officer that many organizations already have in place. Typically, an organization will have such a person dedicated to business IT security. “The most effective way is to expand the accountability and responsibility of that person to now also have oversight of the industrial manufacturing networks as well,” she says. Such expansion of duties is only recently being made, according to Antova, but it’s a necessary step.

As Saadi Kermani, business development manager for Wonderware at Schneider Electric, puts it, “If it’s no one’s job, it’s everyone’s problem.”

That includes the business side of any organization, according to Donovan Tindill, senior security consultant at Honeywell Process Solutions. “Security is synonymous with reliability, and those who prioritize cybersecurity will have a competitive advantage,” he says. In other words, bad security is bad for business.

After making sure that proper responsibility and oversight is assigned for OT security, the next step is to go after what Simonovich calls the low hanging fruit of cybersecurity: making sure that industrial control systems are properly patched with the latest software fixes from their vendors. As he points out, one reason the WannaCry ransomware attack was so devastating was because many of the affected organizations were using old systems without the latest patches. “They were not updating and patching as often as they should,” he says of the victims. “And that vulnerability was left wide open—well documented, well fixed, but ignored.”

As for installing patches, OT systems present special challenges because they cannot be shut down suddenly without negatively impacting the processes they’re running. “There are a handful of critical devices that probably can't be patched without some downtime,” says Jaime Foose, head of the lifecycle support and security solutions organization for Emerson Automation Solutions’ power and water business.

The solution to patching these critical systems is to plan carefully. “You look to do that in an outage window,” Foose says. “You take a short outage, do it in the middle of the night, or a time where it's least disruptive to the process.” With proper preparation, she says, systems can be patched and rebooted in a controlled manner that doesn’t interfere unduly with the processes they control.

In addition to patching, basic security steps normally undertaken in the business IT world can also help secure industrial systems. Implementing user account controls, installing malware protection—including antivirus software and whitelisting-approved access points to prevent unauthorized access—are all among the measures Emerson recommends. “Those very basic things that are common on our home computers and on our work computers are things that in an industrial control environment are sometimes not adopted,” Foose explains.

In all, Foose breaks down best practices for OT cybersecurity into four broad categories:

- Analyze your system to map out what is on your networks and where it resides. This will help you plan defenses and plug gaps in security.
- Deploy defenses, including closing open ports and services that aren’t needed, installing patches, installing malware protection and making sure backups are in place and regularly updated in case all else fails.
- Monitor your systems for unusual activity and intrusions. Managing alarms and keeping track of them is vital for this to work.
- Incidence response is the final piece of the puzzle, ensuring that plans are in place for use when something does go wrong—which may include natural disasters and other incidents, not just cyber attacks.

Many of these ideas are relatively easy to follow, Foose says, and they are also codified in cybersecurity standards put out by authoritative sources such as the National Institute of Standards and Technology (NIST). NIST’s Cybersecurity for Internet of Things (IoT) guidance and its Guide to Industrial Control Systems (ICS) Security point the way to more secure systems, Kermani adds.

Lessons from NERC

Of special interest to critical infrastructure is NERC’s critical infrastructure protection (NERC CIP) guidelines.

If there’s one organization in North America that is especially well equipped to guard against outages cause by cyber attacks and everything else, it’s NERC, which has 50 years of experience keeping the

	North American electric grid online. NERC's chief security officer, Marcus Sachs, is unequivocal in his insistence that critical OT systems should remain isolated. "Our standards make that real clear," he says. "Automate all that you want, but thou shalt not let thy automation touch the Internet." Though NERC standards don't dictate how systems should be built, he says, "We don't want there to be a connection to the Internet. That's the standard." Sachs isn't against connectivity within an OT environment, whether it's at a plant or remotely to engineers monitoring it—just against linking it up willy nilly to the outside world. "If you cross-connect the system with the wide open, public, unregulated, wild, wild West that we call the Internet, you run into problems," he says. After securing access to the broader Internet, Sachs says best practices call for doing away with a monoculture of connectivity. In other words, if every plant is engineered too similarly to others, it gives hackers the means to replicate their efforts, allowing them to leverage hacks on one installation to gain access to another. "Get the systems diverse so that if there's failure, it only fails one, maybe two places, but it can't cascade," Sachs advises. "It can't replicate. It can't go to other systems because they're different." Fortunately, he says, the electric grid here in North America is in good shape in this regard. Finally, Sachs says, it's important to recognize that cyber attacks are launched by people—people using cyber tools to do their dirty work, but people nevertheless. At the same time, cybersecurity is also managed by people whose tools are important, but who must remain aware of the dangers and how to counteract them. "It's not devices fighting devices," he emphasizes. "It's people fighting people." It was apparently a well-funded, well-trained group of cyber criminals who were likely to have been working for the Russian government who took down large portions of the power grid in the Ukraine in 2015 and again in 2016, according to analysis in Wired magazine. In the first attack, hackers were able to gain access to systems controlling circuit breakers because logging into them did not use two-factor authentication. This provided the security hole for the attackers to log in with hijacked credentials that did not have to be verified by other means. Though the Ukrainian power plants were back online in a matter of hours after the first attack, and within an hour following the second, a clear shot had been fired across the bow of the world's industries. The takeaway lesson is that cybersecurity for OT cannot be taken for granted.
Return to Top	

HEADLINE	**11/07 Canada police frustration w/cybercrime**
SOURCE	**https://www.itworldcanada.com/article/canadian-police-frustration-over-cyber-crime-shows-at-conference/398528**
GIST	OTTAWA – Police frustration of dealing with the ever-increasing amount cyber crime businesses and citizens face compared with limited law enforcement resources burst out for a few minutes at a conference here Monday when a senior RCMP officer said more has to be done on prevention. "We're not going to be able to put these things (cyber crime) through the courts and expect to solve it," Scott Doran, director general for federal policing for criminal operations including online crime, told an international cyber crime police summit here. "So, how much effort are we as putting into prevention as a law enforcement community? … I don't think we're doing enough." The Mounties' cyber strategy includes reducing the impact and victimization of cyber crime by identifying and prioritizing threats. But, Doran said, "we're probably not doing a great job … The reality is we don't have the resources. We 're so busy responding that to get out ahead of the thing is very, very difficult." "We do a good job when we get our hands on a 'meaty file' and are able to pursue it,' but we have to

	select highest priority files." He and other police officers who spoke suggested that the public may have to lower expectations about the ability of Canadian police to solve every cyber-related complaint they file. Police forces have to "get our best propeller heads together to solve this issue. We can do it, provided we set expectations and we put our best foot forward and we have a common message." In 2014 the RCMP fielded 7,965 complaints of cyber crime, he said. That rose to were 9,217 a year later and 11,518 in 2016. That doesn't include reports to other forces or the Canadian Anti-Fraud Centre. In an interview later Doran expanded on his comments. "I think we're doing a great job with the capability and capacity we have … At the end of the day what we're probably not doing enough of… is to make more Canadians aware of the threat of cyber crime."
Return to Top	

HEADLINE	**11/07 Electric industry facing cyber alert**
SOURCE	**https://www.ft.com/content/1fc89bd8-996c-11e7-8c5c-c8d8fa6961bb**
GIST	The spear-phishing email attack on US electricity companies in September, allegedly by North Korea, was yet another in a growing barrage of cyber incidents faced by the power generating, transmission and supply industry around the world. "We saw intrusion attempts against US electricity providers from actors that we believe are affiliated with the North Korean government," says John Hultquist, director of intelligence analysis at US cyber security company FireEye, which stopped the emails. Mr Hultquist believes the fake emails, targeted at senior management, could have been a first step to infiltrate the companies' information technology networks, and from there gain access to their industrial control systems. Industrial control systems were hacked in the Ukrainian power grid in December 2016, resulting in power cuts in Kiev lasting more than an hour. Malware called Industroyer was used to control electricity substation switches and circuit breakers, according to Slovakian IT security company ESET. "We believe it was used in the attack on Ukraine's power grid," says Robert Lipovsky, a senior malware researcher at ESET. "It's impossible to say who created it, but it was not the work of a typical cyber criminal, but a group of well-funded and well-motivated people, so state-funded is one possible explanation." The FBI and Department of Homeland Security issued a warning to US infrastructure companies in October following attacks on the electrical power sector and other industries. "The energy sector, being a critical lifeline sector, is targeted by a variety of adversaries," says Mark Bristow, a deputy director at the National Cybersecurity and Communications Integration Centre of the DHS. "We can dispatch an on-site response team once an incident has been reported. We can also hunt for intrusions the energy company might not have detected." Hacking the power grid is more complex than simply infiltrating a computer network. "The grid is designed to be resilient against all sorts of threats and can withstand attacks that are man-made or a result of natural events," says Marcus Sachs, chief security officer of the North American Electric Reliability Corporation, which sets the security standards for the region's power grids. "In fact, there have been no outages or disruptions to the bulk power system in North America due to a cyber attack." Rosa Kariger, chief information security officer for Iberdrola, the Spanish electricity company, agrees: "Unlike information technology, where daily attacks can be counted in the hundreds, attacks on the

	operational technology infrastructure are not easy to execute with success — connectivity is less exposed, system architecture is built upon several layers and electric grids and power plants are designed with sufficient redundancy to withstand a sudden component failure." However, she adds that attackers continue to target critical infrastructure. "These kinds of threats are increasing as cyber sabotage, or even cyber warfare, is becoming more and more the weapon of choice for state- or terrorist-sponsored groups," she says. Leo Simonovich, a cyber strategy expert at Siemens, the German company which provides security solutions to energy companies, agrees: "We see operational technology cyber risk as the new risk frontier." The growing number of web-connected devices in homes, such as domestic heating systems and "smart meters", are also vulnerable to attack, says Dexter Casey, chief information security officer for Centrica, the British electricity and gas supply company. "It's highly unlikely you could launch a successful attack against a generating or grid company via the internet of things, but there's still a risk to the industry's reputation," he says. Consequently, "we spend millions hacking into smart meters to test them," says Mr Casey. A shortage of skilled security staff is a concern for the industry. "I would like to see more apprenticeships, on-the-job-training and university courses structured to get people into the energy industry," says Lawrence Slade, chief executive of Energy UK, the trade association. Some observers fear that the trend away from large, centralised, power stations and towards decentralised power — such as small, flexible gas power plants and solar panels on homes — could increase cyber risk as small power producers would have less sophisticated cyber defences. Mr Slade believes the opposite. "In some respects, moving into a more decentralised world gives you more flexibility and it could be seen as more resilient," he says. Nevertheless, the European Commission has grown concerned about attacks on the energy sector. Its new cyber security package, announced in September, which covers all areas of the EU economy and society, includes proposals for more scrutiny of the software and other components used to monitor industrial control systems. "As we increasingly rely on online technologies," says Sir Julian King, EU commissioner in charge of security issues, "our critical infrastructure such as energy grids, satellite communications and healthcare systems become evermore vulnerable."
Return to Top	

HEADLINE	**11/07 Cost cybercrime rising, attacks increasing**
SOURCE	**https://www.ft.com/content/56dae748-af79-11e7-8076-0a4bdda92ca2**
GIST	Shipping containers could not be booked, lawyers were locked out of their laptops and a production line was prevented from churning out chocolates, as serious cyber attacks swept through major companies earlier this year. Large multinationals from Mondelez to Moller-Maersk, Reckitt Benckiser to FedEx, were forced to warn shareholders that the 'NotPetya' cyber attack had hit their bottom line, costing each company hundreds of millions of dollars. They said that the extent of the damage to their finances was not yet known but projected that the year's revenue would be hit. The rapidly spreading attack highlighted that what matters for most corporate boards is the cost. Never mind the stories of shady criminals, nation state hacking factories and dark web marketplaces packed with stolen data, this is about the bottom line.

Charles Carmakal, vice-president at Mandiant, part of FireEye, has personally responded to hundreds of breaches. He said some companies are still conducting postmortems to figure out the impact of NotPetya. The June attack, which exploited a vulnerability in Ukrainian accounting software, ended up being much more extensive than WannaCry, a ransomware worm that swept through systems in May.

"It was a state sponsored attack against Ukrainian business and way of life but non-Ukrainian victims were likely collateral damage," he said. "Most of the cost is the loss of business, the inability to generate revenue but obviously there are possibly millions of dollars worth of IT costs for rebuilding systems."

The price of a cyber attack varies significantly depending on the kind of breach a company suffers, a company's size, industry and country, and how well prepared it was for an attack. Overall, the cost of cyber security for companies rose 22.7 per cent last year to an average of $11.7m, mainly due to a rising number of security breaches. The number of breaches is up an average 27.4 per cent year on year, according to the Ponemon Institute's Cost of Cyber Crime report. The report was based on 2,182 interviews from 254 companies in seven countries.

The most extensive research has been done on the cost of data breaches, the theft of customer information by hackers, as in the US credit rating company, Equifax hack, where the personal information including social security numbers of 144m Americans were stolen, as well as thousands of UK customers, and the Yahoo breach, where details for over a billion accounts were hacked.

This year, the average cost of a data breach fell from $4m last year to $3.6m, partly because of a strong US dollar, according to a report on data breaches by the Ponemon Institute. The cost of losing each record went down — from $158 to $141 per record — but companies did experience larger breaches, where they lost more records.

However data breaches are just one type of attack. Cyber criminals can embark on distributed denial of service attacks, taking a business offline, and nation state actors are stealing intellectual property.

"One client told me intellectual property they valued at $1bn was stolen," Mr Carmakal said. "That's a real loss if someone else ends up leveraging the data."

Larry Ponemon, founder of the Ponemon Institute, said hackers are increasingly adopting destructive techniques, which leave the business without its valuable data. Ransomware attacks, where hackers encrypt computer files and demand a ransom in return for releasing the decryption key, doubled in frequency in the last year to make up 27 per cent of all incidents.

"The ransomware attacks are the start of something that is a lot more sinister," Mr Ponemon said, adding that criminals could infect industrial control systems, creating huge outages unless companies pay a ransom. "Cyber extortion is the next big wave."

Other cyber security experts warn that hackers could create chaos by not stealing or destroying data, but inserting the wrong data into the system, forcing companies to question the integrity of their records.

Return to Top

HEADLINE	**11/07 Charities unprepared for cyberattack risk**
SOURCE	**https://www.ft.com/content/1c9ad7a0-996c-11e7-8c5c-c8d8fa6961bb**
GIST	In January 2017, Little Red Door, a small US healthcare charity, received an ominous email with "Cancer Sucks, But We Suck More!" as the subject line. Hackers had blocked access to the client files and financial data of the Indiana-based organisation and were demanding money for its release. Little Red Door opted not to pay the bitcoin ransom (equivalent to about $43,000), as it did not keep sensitive information, such as bank account details or social security numbers. However, it had to spend

	months rebuilding its client data. The size of the charity and its social mission — providing services to people in its area who have a cancer diagnosis — showed how undiscriminating cyber criminals can be in choosing their target. Yet while the chances of being hacked are as high for a charity as for any other organisation, the non-profit sector is unprepared to meet cyber threats. In a 2016 survey by US accounting firm CohnReznick, almost half of the non-profit organisations polled said they had not completed a cyber-risk assessment in the past year and 66 per cent had no plan to increase their spending on data security. While it is not surprising that charities want to spend scarce resources on housing the homeless or feeding the hungry, some argue that those very services could be at risk if they fail to invest in cyber security tools and practices. Part of the problem is that non-profit organisations do not put a price on not being able to operate, says Ken Montenegro, IT director at advocacy group Asian Americans Advancing Justice. "Non-profits don't have a good analysis of down time," says Mr Montenegro, who is part of a cohort of IT directors from advocacy organisations who collaborate on cyber security. In addition, he says, IT budgets are often spent on areas such as communications, seen as key to fundraising, rather than cyber security. "That puts us in a precarious position because we're not used to spending on something like a patch management tool that keeps our software up to date," he says. However, the costs of being unprepared can be high, something charities can ill afford. When breached by ransomware, the potential human cost of being unable to deliver services means the pressure for non-profit organisations to pay off the hackers is intense. Last year, for example, a Los Angeles non-profit hospital paid a bitcoin ransom equivalent to about $17,000 to regain access to the medical records of its patients after hackers attacked parts of its network. Statistics on the number of charities being hacked are hard to obtain, since many organisations do not report these incidents. However, in the rising tide of cyber crime — which research company Cybersecurity Ventures predicts will cost the world $6tn a year by 2021 — non-profit organisations are certainly not excempt. Nor is it only the data of the clients they serve that charities need to worry about. As online giving has swept through the non-profit sector, it has also created new risks. Because they permit very small donations to be made online, for example, non-profits are frequently the target of credit card fraudsters who use donation forms to check if stolen credit card details will work. "As long as there have been online donations, there's been online donation fraud," says Steve MacLaughlin, vice-president of data and analytics at Blackbaud, which provides non-profit organisations with software and services.
Return to Top	

HEADLINE	**11/08 FBI: church shooter's phone 'locked'**
SOURCE	**https://apnews.com/417c7d792699442e831663a3e9139637/FBI-again-finds-itself-unable-to-unlock-a-gunman's-cellphone**
GIST	WASHINGTON (AP) — The Texas church massacre is providing a familiar frustration for law enforcement: FBI agents are unable to unlock the gunman's encrypted cellphone to learn what evidence it

might hold.

But while heart-wrenching details of the rampage that left 26 people dead might revive the debate over the balance of digital privacy rights and national security, it's not likely to prompt change anytime soon.

Congress has not shown a strong appetite for legislation that would force technology companies to help the government break into encrypted phones and computers. And the fiery public debate surrounding the FBI's legal fight with Apple Inc. has largely faded since federal authorities announced they were able to access a locked phone in a terror case without the help of the technology giant.

Still, the issue re-emerged Tuesday, when Christopher Combs, the special agent in charge of the FBI's San Antonio division, said agents had been unable to get into the cell phone belonging to Devin Patrick Kelley, who slaughtered much of the congregation in the middle of a Sunday service.

"It highlights an issue you've all heard about before. With the advance of the technology and the phones and the encryption, law enforcement is increasingly not able to get into these phones," Combs told reporters. He did not provide further details other than saying the device was being flown to an FBI lab for analysis. "We're working very hard to get into that phone, and that will continue until we find an answer," Combs added.

Combs was telegraphing a longstanding frustration of the FBI, which claims encryption has stymied investigations of everything from sex crimes against children to drug cases, even if they obtain a warrant for the information. Agents have been unable to retrieve data from half the mobile devices — more than 6,900 phones, computers and tablets — that they tried to access in less than a year, FBI Director Christopher Wray said last month, wading into an issue that also vexed his predecessor, James Comey. Comey spoke before Congress and elsewhere about the bureau's inability to access digital devices. But the Obama White House never publicly supported legislation that would have forced technology companies to give the FBI a back door to encrypted information, leaving Comey's hands tied to propose a specific legislative fix.

Security experts generally believe such encryption backdoors are a terrible idea that could expose a vast amount of private, business and government data to hackers and spies. That's because those backdoor keys would work for bad guys as well as good guys — and the bad guys would almost immediately target them for theft, and might even be able to recreate them from scratch.

Deputy Attorney General Rod Rosenstein took aim at Silicon Valley's methods for protecting privacy during a speech last month, saying Trump's Justice Department would be more aggressive in seeking information from technology companies. He took a harder line than his predecessors but stopped short of saying what specific steps the administration might take.

Washington has proven incapable of solving a problem that an honest conversation could fix, said David Hickton, a former U.S. attorney who now directs a cyberlaw institute at the University of Pittsburgh.

"We wait for a mass disaster to sharpen the discussion about this, when we should have been talking about it since San Bernardino," he said. "Reasonable people of good will could resolve this problem. I don't think it's dependent on the political wins or who is the FBI director. It's begging for a solution."

Even so, the facts of the church shooting may not make it the most powerful case against warrant-proof encryption. When the FBI took Apple to court in February 2016 to force it to unlock the San Bernardino shooter's phone, investigators believed the device held clues about whom the couple communicated with and where they may have traveled.

But Combs didn't say what investigators hoped to retrieve from Kelley's phone, and investigators already have ample information about his motive. Authorities in Texas say the church shooting was motivated by the gunman's family troubles, rather than terrorism, and investigators have not said whether they are seeking possible co-conspirators.

	Investigators may have other means to get the information they seek. If the Texas gunman backed up his phone online, they can get a copy of that with a legal order — usually a warrant. They can also get warrants for any accounts he had at server-based internet services such as Facebook, Twitter and Google.
Return to Top	

HEADLINE	**11/07 Twitter doubles character limit to 280**
SOURCE	**https://www.washingtontimes.com/news/2017/nov/7/twitter-doubles-character-limit-to-280-for-nearly-/**
GIST	NEW YORK (AP) — Twitter says it's ending its iconic 140-character limit - and giving nearly everyone 280 characters. Users tweeting in Chinese, Japanese and Korean will still have the original limit. That's because writing in those languages uses fewer characters. The company says 9 percent of tweets written in English hit the 140-character limit. This causes people to spend more time editing their tweets or not sending them out at all. Twitter hopes that the expanded limit will get more people tweeting more, helping its lackluster user growth. Twitter has been testing the new limit for weeks and is starting to roll it out Tuesday. The company has been slowly easing restrictions to let people cram more characters into a tweet. It stopped counting polls, photos, videos and other things toward the limit.
Return to Top	

HEADLINE	**11/07 Drive-by cryptomining hassles visitors**
SOURCE	**https://www.infosecurity-magazine.com/news/driveby-cryptomining-hassles/**
GIST	Drive-by crypto-mining is digging into the web, victimizing unsuspecting visitors to some websites by utilizing 100% of their CPU to mine for cryptocurrency with no knowledge or consent given. According to analysis from Malwarebytes, a company called Coinhive launched a service back in September that could mine for the digital currency known as Monero from directly within a web browser, using JavaScript-based code. The mining API is cross-platform compatible and works on all modern browsers. In and of itself, the technology offers a potential new revenue stream for website owners, perhaps replacing annoying banners and pop-ups with small slowdowns in computer performance stemming from the mining activity. It could be, in theory, a win-win. There's just one problem: the technology was almost instantly abused. "The simplicity of the Coinhive API integration was one of the reasons for its immediate success…[but] many web portals started to run the Coinhive API in non-throttled mode, resulting in cases of cryptojacking," explained Malwarebytes analyst Jerome Segura. "While the harm may seem minimal, this is not the kind of web experience most people would sign up for. To make matters worse, one does not always know if they are mining for the website owner or for criminal gangs that have found a new monetization tool for the hacked sites they control." The scale of drive-by mining activity is not minor, either. Malwarebytes has been blocking the original Coinhive API and related proxies an average of 8 million times per day, Segura said, which adds up to approximately 248 million blocks in a single month.
Return to Top	

HEADLINE	**11/08 Russia-linked spies exploit DDE**
SOURCE	**http://www.securityweek.com/russia-linked-spies-deliver-malware-dde-attack**
GIST	The Russia-linked cyber espionage group tracked as APT28 and Fancy Bear has started delivering malware to targeted users by leveraging a recently disclosed technique involving Microsoft Office documents and a Windows feature called Dynamic Data Exchange (DDE). Researchers at McAfee noticed the use of the DDE technique while analyzing a campaign that involved blank documents whose name referenced the recent terrorist attack in New York City. Researchers warned recently that DDE, a protocol designed for data exchanges between Windows applications, could be used by hackers as a substitute for macros in attacks involving malicious documents. Shortly after, security firms reported seeing attacks leveraging DDE to deliver malware, including Locky ransomware. Microsoft pointed out that DDE, which has been replaced with Object Linking and Embedding (OLE), is a legitimate feature. The company has yet to make any changes that would prevent attacks, but mitigations included in Windows do provide protection, and users are shown two warnings before the malicious content is executed. In the APT28 attacks spotted by McAfee, cyberspies used the document referencing the New York City attack to deliver a first-stage malware tracked as Seduploader. The malware, typically used by the threat actor as a reconnaissance tool, is downloaded from a remote server using PowerShell commands. Based on the analysis of the malware and command and control (C&C) domains used in the attack, researchers determined that the campaign involving DDE started on October 25. The attack using the New York City incident as lure appears to be part of a campaign that also involved documents referencing Saber Guardian, a multinational military exercise conducted by the U.S. Army in Eastern Europe in an effort to deter an invasion (by Russia) into NATO territory. Another recent APT28 attack leveraged a document describing CyCon U.S., a conference organized by the NATO Cooperative Cyber Defence Centre of Excellence (CCDCOE) in collaboration with the Army Cyber Institute at West Point. However, the CyCon attack relied on a malicious VBA script and it did not involve DDE.
Return to Top	

HEADLINE	**11/07 Texas Nat'l Guard $373K on stingray**
SOURCE	**https://www.scmagazine.com/texas-national-guard-used-stingrays-on-surveillance-planes/article/705830/**
GIST	The Texas National Guard last year spent more than $373,000 to install two of its DRT 1301C "portable receiver systems" in two RC-26 surveillance aircraft. The Texas Observer obtained a contract between Digital Receiver Technology Inc., or DRT, the manufacturers of the device, and the Texas National Guard stating the stingrays were for "investigative case analytical support" in counternarcotics operations and were purchased using state drug-asset forfeiture money. Unlike older stingray devices, the DRT 1301C are capable of capturing all of the content transferred from a user's device, Austin attorney Scott McCollough who serves on the board of the Austin chapter of Electronic Frontier Foundation told the publication. At one point the surveillance planes reportedly operated under a front company named Air Cerberus, but have since been converted to military registrations.

Return to Top	

HEADLINE	**11/07 Pro-ISIS hackers hijack school sites**
SOURCE	**https://www.scmagazine.com/hundreds-of-school-websites-redirected-pro-isis-web-page/article/705985/**
GIST	Pro-ISIS hackers hijacked the websites of roughly 800 U.S. schools and educational districts on Monday, after compromising their web hosting provider, various news outlets have reported. The hacking group Team System Dz claimed responsibility for the cyberattack, which redirected users to a website displaying ISIS messages and a recruitment video, as well as an image of former Iraqi president Saddam Hussein, according to the International Business Times UK. The websites' hosting services provider, Atlanta-based SchoolDesk, reportedly confirmed the attack, noting in a statement that it responded to the incident "immediately" by taking down the impacted websites. "Our technical staff discovered that a small file had been injected into the root of one of the SchoolDesk websites, redirecting approximately 800 school and district websites to an iFramed YouTube page containing an audible Arabic message, unknown writing and a picture of Saddam Hussein," the statement reads. "Although the exact method and point of intrusion is not yet fully known (possibly an SQL injection or through a user account with a weak password), we have added multiple layers of redundant protection to prevent this from happening again, as well as taking many additional methods to research how this was accomplished and by whom." The IBT UK further reports that educational districts in Connecticut, Louisiana, New Jersey, and Virginia were affected. In June, Team System DZ attacked government websites in Ohio, Maryland and New York, defacing them with a pro-ISIS message that read, in part, "I Love Islamic state." The hackers used the same phrasing in the school cyberattack.
Return to Top	

HEADLINE	**11/07 Phony Netflix email phishing scam**
SOURCE	**https://www.scmagazine.com/another-netflix-phishing-scam-looking-to-steal-payment-info/article/706004/**
GIST	Another Netflix phishing campaign was seen in the wild prompting customers to update their login credentials or risk being locked out of their account. A similar scam occurred earlier this year. Mailguard researchers described the email used in the scam as being relatively well designed and said the scammers are using a template system to generate individualized messages with specific recipient data, according to a Nov. 3 blog post. While the body of the email is generic, the sender field is designed to show the name of the victim personalizing the message more so it seems more convincing. The emails subject line reads “Your suspension notification” and is addressed “Hi #name#.” “We are unable to validate your billing information for the next billing cycle of your subscription therefore we'll suspend your membership if we don't not receive a response from you within 48hours,” the message said. “Obviously we'd love to have you back, simply click restart your membership to update your details and continue to enjoy all the best TV shows and movies without interruption.” The message features a restart membership button along with phony links to contact the company and for a

	help center. It's unclear how many people were affected by the scam. Votiro Security Researcher Amit Dori said users should think before they click and examine emails before responding.
Return to Top	

HEADLINE	**11/07 Flaw locks out $300M cryptocurrency**
SOURCE	**https://thehackernews.com/2017/11/parity-ethereum-wallet.html**
GIST	About $300 million worth of Ether—the cryptocurrency unit that has become one of the most popular and increasingly valuable cryptocurrencies—from dozens of Ethereum wallets was permanently locked up today. Smart contract coding startup Parity Technologies, which is behind the popular Ethereum Parity Wallet, announced earlier today that its "multisignature" wallets created after this July 20 contains a severe vulnerability that makes it impossible for users to move their funds out of those wallets. According to Parity, the vulnerability was triggered by a regular GitHub user, "devops199," who allegedly accidentally removed a critical library code from the source code that turned all multi-sig contracts into a regular wallet address and made the user its owner. Devops199 then killed this wallet contract, making all Parity multisignature wallets tied to that contract instantly useless, and therefore their funds locked away with no way to access them. Parity multisignature wallets also experienced a vulnerability in July this year that allowed an unknown hacker to steal nearly $32 million in funds (approximately 153,000 units of Ether) before the Ethereum community secured the rest of its vulnerable Ether. According to Parity, a new version of the Parity Wallet library contract deployed on 20th of July contained a fix to address the previously exploited multi-sig flaw, but the code "still contained another issue," which made it possible to turn the Parity Wallet library contract into a regular wallet.
Return to Top	

HEADLINE	**11/07 Study: most firms run old Office software**
SOURCE	**https://www.infosecurity-magazine.com/news/most-organizations-run-outofdate/**
GIST	Over two-thirds of organizations are running unsupported versions of Microsoft Office, exposing them to cyber-threats, according to a new study from Spiceworks. The IT professional network polled over 1,100 IT pros in the US, Canada and UK to better understand the usage of productivity suites in their organizations. It found 68% are still running some instances of Office 2007, despite the package reaching end of support in October this year. The bad news doesn’t end there: 46% were running Office 2003; 21% Office 2000; and 15% are still on Office XP (2002 version). Some 3% even claimed they are still running some machines on Office 97. “Although they might not grab as many headlines as end-of-support OSes, Office suites that are past their prime are susceptible to danger, similar to their OS cousins,” explained Spiceworks senior technology analyst, Peter Tsai. “Just like any software or system in use, productivity suites need to be patched for security reasons. Once an OS no longer receives updates, it's a security liability. Over the years, there have been hundreds of

	vulnerabilities identified in Microsoft Office." If organizations need reminding of the damage that can result from an unpatched vulnerability, they just need to look at the chaos inflicted by WannaCry and NotPetya, two worm-like ransomware threats that caused mass service outages across the globe in May and June.
Return to Top	

HEADLINE	**11/07 Scottish charity leaks data on vulnerable**
SOURCE	**https://www.infosecurity-magazine.com/news/info-vulnerable-adults-victims/**
GIST	The website of a Scottish charity which works with some of society's most vulnerable members has been shut down after a major data leak was revealed, exposing sensitive information on around 50 people. The Scottish Appropriate Adult Network (SAAN) works to safeguard the interests of children or vulnerable adults that have been arrested or called in for questioning by the police. It does this by providing so-called "appropriate adults" to accompany and offer support to these individuals during the process. However, scores of these volunteers and vulnerable adults had their personal details including names, email addresses and phone numbers exposed by the SAAN website, *The Sunday Post* reported. Also apparently included on the site was information about rape victims and domestic abuse cases. To make matters worse, SAAN was contacted last year about the privacy snafu but failed to respond — apparently because of the same issue with the site. "As soon as we were notified of the difficulties, we took immediate action and the website is unavailable until the issue has been resolved," SAAN interim chair, Karen Donoghue, told the paper. The ICO is said to be investigating the case.
Return to Top	

HEADLINE	**11/06 What happened to GozNym Trojan?**
SOURCE	**https://www.scmagazine.com/where-are-they-today-banking-trojans-that-no-one-misses-goznym--up-a-storm-then-up-in-flames/article/705384/**
GIST	According to IBM X-Force data, several major cybercrime groups that operate banking Trojans have slowly relinquished center stage in 2017, and for no apparent external reason. These groups include: Shifu, Tinba, Neverquest, Qadars, and GozNym – all of which have gradually faded away, or are nearing hiatus in 2017. Where were these malware codes before, and where are they today? This blog series reviews their history and tracks the current status of each Trojan. In this blog post, we focus on GozNym. The GozNym Trojan was an interesting case when it emerged in April 2016. Upon its detection, IBM X-Force research analyzed it and reported that it was actually not one, but two malware codes meshed into one. A two headed beast made of a powerful infector in the shape of the Nymaim loader, and a proven bank fraud module that came from Gozi ISFB. GozNym's operators did not waste any time. They took this new code and started attacking banks in the US. Within a matter of days, they had already managed to steal millions of dollars, and that was only the beginning.

	Within the span of one week, GozNym started attacking in Poland, a different language zone and different banking system than the one used in the U.S. It meant that this was a group, and to top it off, the malware featured redirection attacks – a sophisticated way to take victims to a fake site, away from the bank's security and detection, and take over their accounts. There was no doubt that this malware's operators knew what they were doing, and have been preparing for a while. The next step was bringing the redirection scheme to US business banking in June 2016. By August 2016, GozNym was equipped with redirection attacks that targeted German banks, intensifying its attacks in Europe in peaks of thousands of percentage points comparing the four months prior. With its forceful launch and rapid spread, GozNym got the attention of banks, security teams, and law enforcement alike. It was at its peak right when a new contender showed up in the cybercrime arena – the TrickBot Trojan – starting to chomp chunks of GozNym's turf, redirection attacks and all. By summer of 2016, it was clear that GozNym was a new force in the cybercrime arena. In November 2016, X-Force research was still observing campaigns in the US and in Germany. Possibly operated by two actors/groups in tandem, in Germany the malware continued to focus on bank accounts, whereas in the US, GozNym had diversified its target list for the Holiday Season. It added the top most popular electronics retailers, ecommerce sites, eWallet providers, telecommunications vendors, and payment card providers to the target list, and launched a new infection campaign. And while all this was happening, something else was underway behind the scenes – the upcoming takedown of the largest and longest standing bulletproof cybercrime operations that just happened to also host GozNym attacks: the Avalanche network. The Europol released notice about the takedown on Dec.1, 2016. And on Dec.12, 2016, the American DoJ released a notice on the arrest of a Bulgarian national charged with operating GozNym attacks against US residents. The six-count indictment was being prepared for months previous, and although it only came up with a sole defendant, unsealing the indictment provided a rare glimpse into the sort of money banking Trojan operators steal from organizations they target. The amounts reported by the DoJ ranged $118,000 to $737,000 from each victim, and GozNym was just getting started. Other, longer standing groups like Dridex, have already been named as the culprits in losses of millions of dollars at a time. After his arrest, the alleged captured GozNym gangster was facing 100 years in US prison. An indictment that sent a clear message to the group: things just got real. The investigation and arrest of one of its members affected the GozNym gang enough to have its operation halted.
Return to Top	

HEADLINE	**11/07 Marcher banking Trojan targets Austria**
SOURCE	**https://www.scmagazine.com/marcher-banking-trojan-campaign-attacks-austrians-finances-three-different-ways/article/705712/**
GIST	An attack campaign targeting Android users in Austria has been employing a unique trio of techniques to steal their funds: a credentials phishing web page, malicious banking app overlays, and credit card phishing screens. The latter two techniques come courtesy of the Marcher banking trojan, which, according to a Proofpoint blog post published last Friday, is being used in increasingly sophisticated campaigns, "with multiple attack vectors and various targeted financial services and communication platforms." Proofpoint notes that the three-in-one Marcher campaign has been active since at least January 2017,

	setting its sights on customers of large Austrian financial institutions such as Bank Austria, Raiffeisen Meine Bank, and Sparkasse. Unlike many other Marcher attacks that have used SMS to spread, the Austrian campaign relies on malspam emails that typically use a bit.ly shortened malicious links to direct users to a phishing landing page that imitates a particular bank, asking for login credentials or an account number and PIN. If the victim complies, he or she is then asked to log in with their email address and phone number. These phishing pages generally resolve to domains that incorporate the bank's name, in order to further exude credibility. Once users enter their information into the phishing page, thereby giving away their information to the cybercriminals, the Marcher phase of the attack begins. The victims are falsely informed via the malicious mobile web page that they do not have their bank's security app installed on their phones, and must download it in order to comply with new European Union money laundering guidelines as well as to encrypt sensitive data such as mTan SMS and online banking connections. In the case of a fake BankAustria security app used in a Nov. 2 campaign, Proofpoint found that 7 percent of visitors were socially engineered into downloading this so-called "application," which is actually the Marcher banking trojan. Proofpoint further warns that the faux security application asks for a wide range of suspicious permissions that would elevate Marcher's privileges and give it increased control over the infected device. Chief among these is the request to act as device administrator. Later, when the victim opens up a specific banking app, Marcher attacks in its usual manner, by overriding the app's true screen with a fake overlay that imitates the bank and steals the user's credentials information as it's being entered. It might seem redundant for the cybercriminals to employ Marcher in this manner if the initial phishing attack already captured the victim's credentials in phase one of the attack. But not so -- because unlike with phishing attacks, Marcher can repeatedly harvest victims' credentials even after they are changed, explained Patrick Wheeler, director of threat intelligence at Proofpoint, in an email interview. Moreover, banking trojans like Marcher often target "multiple banks and financial services, so even if victims turned over credentials for one bank, the trojan may be able to harvest credentials for others as they use their phones," Wheeler added. In what constitutes a third method of attack, the Marcher trojan in this particular case also presented credit card phishing screens when users opened non-banking apps such as the Google Play Store.
Return to Top	

HEADLINE	**11/07 Gaming keyboard w/built-in keylogger**
SOURCE	**https://thehackernews.com/2017/11/mantistek-keyboard-keylogger.html**
GIST	"The right keyboard can make all the difference between a victory and a defeat in a video game battlefield." If you are a gamer, you can relate to the above quote. But what if your winning weapon betrays you? The popular 104-key Mantistek GK2 Mechanical Gaming Keyboard that costs around €49.66 has allegedly been caught silently recording everything you type on your keyboard and sending them to a server maintained by the Alibaba Group. This built-in keylogger in Mantistek GK2 Mechanical Gaming Keyboard was noticed by a few owners

	who headed on to an online forum to share this issue. According to Tom's Hardware, MantisTek keyboards utilise 'Cloud Driver' software, maybe for collecting analytic information, but has been caught sending sensitive information to servers tied to Alibaba. The affected users also provided a screenshot showing how all your plain-text keystrokes collected by the keyboard are being uploaded to a Chinese server located at IP address: 47.90.52.88. However, since like Amazon and Google, Alibaba Group also sells cloud services, this collected information is not necessarily being sent to the Alibaba itself, but someone who is using the company's service.
Return to Top	

HEADLINE	**11/07 'Sowbug' stealing diplomatic secrets**
SOURCE	**https://thehackernews.com/2017/11/sowbug-hacking-group.html**
GIST	A previously unknown hacking and cyber-espionage group that has been in operation since at least 2015 have conducted a series of highly targeted attacks against a host of government organizations in South America and Southeast Asia to steal their sensitive data. Codenamed Sowbug, the hacking group has been exposed by Symantec security researchers, who spotted the group conducting clandestine attacks against foreign policy institutions, government bodies and diplomatic targets in countries, including Argentina, Brazil, Ecuador, Peru and Malaysia. Symantec analysis found that the Sowbug hacking group uses a piece of malware dubbed "Felismus" to launch its attacks and infiltrate their targets. First identified in late March of this year, Felismus is a sophisticated, well-written piece of remote access Trojan (RAT) with a modular construction that allows the backdoor trojan to hide and or extend its capabilities. The malware allows malicious actors to take complete control of an infected system and like most RATs, Felismus also allows attackers to communicate with a remote server, download files, and execute shell commands. By analysing Felismus, researchers were able to connect previous attack campaigns with the Sowbug hacking group, indicating that it had been active since at least early-2015 and may have been operating even earlier. "To date, Sowbug appears to be focused mainly on government entities in South America and Southeast Asia and has infiltrated organizations in Argentina, Brazil, Ecuador, Peru, Brunei and Malaysia," the Symantec report said. "The group is well resourced, capable of infiltrating multiple targets simultaneously and will often operate outside the working hours of targeted organisations." Although it is still unclear how the Sowbug hackers managed to gain a foothold in computer networks, evidence gathered by researchers suggested the hackers have made use of fake, malicious software updates of Windows or Adobe Reader. The researchers also found that the group have used a tool known as Starloader to deploy additional malware and tools, such as credential dumpers and keyloggers, on victims' networks.
Return to Top	

HEADLINE	**11/07 Downloading fake apps; getting hacked**
SOURCE	**http://abcnews.go.com/US/protect-downloading-fake-apps-hacked/story?id=50972286&cid=clicksource_81_2_hero_headlines_headlines_hed**
GIST	A cybersecurity expert is warning smartphone users to be cautious of downloading fake apps that can potentially give hackers unfettered access to the personal information on your phone. In September, hackers introduced dozens of malicious apps onto the Google Play store, also known as “doppelgangers" because these fake apps imitated some commonly used real apps. Unsuspecting Android users downloaded the bad apps a total of 4.2 million times, according to Google Play. ABC News' Gio Benitez and cybersecurity expert James Lyne set up a demonstration at a coffee shop in Washington, D.C. to show how vulnerable people may be when downloading fake apps. Lyne explained that apps are especially malicious because users "don't realize that it's a fake." Benitez explained that apps are especially malicious because users "don't realize that it's a fake." Lyne, who works at the global security firm Sophos, added that many of the bad apps may still seem to work, meaning users may not even be aware that their phone's security has been compromised. "If you download a nasty version of Minecraft, for example, you actually seem to get Minecraft," Lyne said. "And it seems to work, but in the background, the attackers are able to access your information." During the demo, Lyne gave Android phones to five volunteers and asked them to use the phones as they normally would. Unbeknownst to the participants, Lyne had already installed a malicious app, called "Lovely Wallpaper," on their phones. Through the app, Lyne was able to easily hack into the participants' phones without them even knowing. "We could retrieve their text messages," Lyne said, as he and Benitez remotely viewed some text conversations taking place during the demo. Lyne added that he was also able to gain access to the phones' cameras. "He's going to have no idea that the camera just activated," Lyne said during the demo. "There's a photo of one of our users." During the demo, all of the volunteers signed into at least one of their social media accounts on the phones. Lyne was then able to gain access to all of their passwords. When Lyne and Benitez revealed that they had been able to read the group's text messages, steal passwords and even take a photo, the participants were shocked. "Did you take that of me while I was on my phone?" one volunteer, Jeremy Pinson, asked. "That's terrifying." When one volunteer walked around outside of the coffee shop, Lyne was even able to track his location using his phone. "I am tracking him now," Lyne said. "I can see exactly where he is." Lyne said that he could even remotely control the text messages sent from one of the phones that he hacked through the app and added that someone does not even have to be using the phone when it is hacked.

	"Even when you weren't using the phone, we still got a picture of you," Benitez told one volunteer. "The phone was just sitting there on the table looking right up at you." Lyne added that through malicious apps your security may be compromised without you even knowing. "Once a cybercriminal is into your phone, they can access your usernames and passwords and credit cards," ," Lyne said, adding that a criminal could even "be able to profit from your device without you knowing." A Google spokesperson told ABC News in a statement that they have been tracking the malware, known as ExpensiveWall, that was used in "Lovely Wallpaper" and other apps. "We have been closely tracking this malware family for months, and continue to take actions, such as removing apps from Play, when we detect its variants," the spokesperson said. "We are constantly updating Google Play Protect -- our safeguard for all Android devices with Google Play -- to detect malware like ExpensiveWall and secure our users."
Return to Top	

Terror Conditions

Top of page

HEADLINE	**11/07 Bin Laden son seeks revenge on US**
SOURCE	**http://www.dailymail.co.uk/news/article-5058753/Hamza-bin-Laden-speech-father-s-legacy.html**
GIST	Osama bin Laden's 'favourite' son has called on Muslims around the world to launch terror attacks on the US for killing his father. Hamza bin Laden, believed to be around 28 years old, has been hailed as the 'heir' to the leadership of Al-Qaeda after his father was shot dead by SEAL Team Six in 2011. In an audio message released today he urges Muslims to 'to take revenge on the Americans, the murderers of the Shaykh [Osama bin Laden], specifically on those who participated in this heinous crime.' In the message, translated for MailOnline by the Middle East Media Research Institute, Hamza tells young Muslim men to prepare for a new wave of armed uprisings across the Arab world. He also rejects democracy, saying that 'freedom cannot be earned with worthless pieces of paper cast inside a ballot box, nor by participation in polytheistic parliaments which legislate by man-made laws; it's earned with the ultimate generosity, selfless sacrifice… Jihad and martyrdom.' 'Jihad must continue until the preparations are complete and the masses are ready for an uprising, so that the spark of an uprising may finally be lit, for its volcanic eruption to sweep aside the tyrant, liberate the masses from oppression, injustice and humiliation, and establish the Shariah of Allah.' Those who have the capacity for this undertaking may utilize the Shaykh's [Osama bin Laden's] example as an inspiration for rising up against tyrants, changing the corrupt order, repelling the occupation, and returning to their Islamic roots... 'Rise in rebellion against the arrogant tyrants and return to Jihad in the Way of Allah.' This comes just days after Hamza bin Laden's wedding video was released, showing the 'Crown Prince of Terror' as an adult for the first time. This was released by the CIA as part of a trove of material recovered during the May 2011 raid that killed the terror group leader at his compound in Pakistan.

	Until now, the public has only seen childhood photos of Hamza, which have been used as propaganda tools by al Qaeda. It's believed the militants have not released pictures of him as an adult for his own safety. The hour-long video shows Hamza bin Laden, sporting a trimmed mustache but no beard, at his wedding which is believed to have taken place around ten years ago while he was living in Iran under house arrest for several years. It is unclear who the bride is, as Al Qaeda militants - including his own father - take multiple wives, but his marriage to the daughter of senior al Qaeda military leader, Abu Mohammed al-Masri is well documented. Footage of his wedding shows Hamza sitting on a carpet with other men, while a man chanting Koranic verses can be heard in the background. Sporting a traditional white headdress, he verbally accepts his marriage to his bride 'on the book of God and the example of the prophet. Peace be upon him.' 'Takbeer!' the others shout, marking his marriage with a kind of religious hooray. There did not appear to be any obvious security around the event and Hamza and his guests appear to be laughing and singing. It is unclear how Osama bin Laden came to possess his son's wedding tape, shot in Iran, at his secret Abbottabad compound.
Return to Top	

HEADLINE	**11/08 West Africa force faces uphill battle**
SOURCE	**https://www.usnews.com/news/world/articles/2017-11-08/short-on-boots-and-backing-west-africa-force-faces-uphill-battle**
GIST	SEVARE, Mali (Reuters) - Snipers from a new West African force lie prone on a rooftop in central Mali, scanning the horizon for Islamist militants who have infiltrated this sparsely populated region south of the Sahara and made it a launchpad for deadly attacks. Thousands of U.N. peacekeepers, French troops and U.S. military trainers and drone operators have failed to stem a growing wave of jihadist violence, leading international powers to pin their hopes on a new regional force. But the so-called G5 Sahel initiative faces immense challenges if it is to do any better at bringing security to the arid Sahel region than its countries Burkina Faso, Chad, Mali, Mauritania and Niger have managed so far. Security sources and analysts say too strong an emphasis on military might over tackling the underlying causes of jihad, logistical shortfalls and a lack of cooperation from regional powerhouse Algeria all raise doubts over whether the G5 can succeed where years of Western intervention has not. "There is a long way to go to reach full operational capacity, even though the timeframe is relatively short," G5 force commander General Didier Dacko told visiting U.N. Security Council envoys last month, citing a range of needs from aerial support to communications equipment to intelligence gathering. The United Nations, France and the United States have poured billions of dollars into stabilizing the region over the past 15 years but have failed to meaningfully address the many local grievances driving conflict, analysts say. Political and social tensions, such as a stalled peace process between the government and armed groups in

	Mali, are pushing youths to jihad, as are growing rivalries between farmers and cattle herders and rights abuses by national armies. In northern Burkina Faso, for example, preacher Malam Ibrahim Dicko has gained adherents to his militant Ansarul Islam movement by railing against the privileges of traditional elites in a region scarred by widespread poverty. Some local groups have affiliated themselves with global franchises such as al Qaeda and Islamic State, whose dwindling presence in the Middle East has led Western governments to zero in on the vast lawless tracts of North and West Africa to prevent them finding new footholds. But the militant groups in the Sahel draw more on frustrations with central governments and the Western forces that back them than a global jihadist agenda, making security-heavy approaches risky, analysts say. "I think local communities in Mali and Niger feel alienated and confused by the actions of those entities," said Alexander Thurston, an assistant professor at Georgetown University who specializes in Islam and politics in West Africa. "The problems require political solutions, ultimately, and the G5 is a small and underfunded force." France is keenly backing the G5, hoping it will provide an eventual exit strategy for its own costly 4,000-strong counter-terrorism taskforce in the region, Operation Barkhane. "Terrorist groups in the Sahel now represent a global threat," French Foreign Minster Jean-Yves Le Drian told the Security Council last week. "The G5 Sahel joint force is the right response to this challenge." The threat Islamist militants pose was underscored by last month's attack in Niger that killed eight U.S. and Nigerien troops, prompting American officials to predict U.S. involvement in the region would intensify. Joint patrols, hot pursuit operations and intelligence sharing among the five countries contributing to the force, which should eventually boast nearly 5,000 soldiers, will chase out drug traffickers and militants, he said. Neither the U.N. mission in Mali, which cannot operate across borders, nor the French taskforce, which has concentrated on training local forces and going after high value targets, has made securing the region's porous borders a priority. Last week, the G5 deployed its first several hundred troops from Mali, Niger and Burkina Faso to their shared borderlands where jihadists have carried out dozens of attacks this year.
Return to Top	

HEADLINE	**11/08 ISIS turns to social media for support**
SOURCE	**http://www.scmp.com/week-asia/politics/article/2118968/support-islamic-state-indonesia-theres-app**
GIST	Robbing banks, dealing drugs, stealing motorcycles – these are the kind of activities popularly associated with the world of terrorist group funding. But to the modern jihadi they're all a little passé. ATM smash and grabs, thefts and laundering money from front charities may have been all the rage as recently as 2014, but since 2015 online donations have been the avenue of choice for Islamic State supporting groups hoping to finance attacks in Indonesia, the world's most populous Muslim-majority nation. That's according to a new joint study by the country's National Counterterrorism Agency, State Intelligence Agency, and Financial Transaction Reports and Analysis Centre (PPATK), which examined

the banking transactions involved in terror cases between 2014 and August 2017.

"Terror groups now call for donations through social media [and messaging platforms] such as WhatsApp groups or Twitter," said Kiagus Ahmad Badarudin, chairman of the PPATK. "Bitcoin and PayPal are also used to move their money."

Social media appealed to terrorists because it was practical, easy and borderless, Badarudin said. Most donations over social media were small, ranging from US$100-US$1,000, but the flow of aid was continuous and tough to track, he said.

Terror cells were also receiving contributions from legal businesses such as small-scale merchants and phone credit sellers, Badarudin added.

The shift online was, in part, due to a tightening of the net by security services.

"Jemaah Islamiyah in particular used a network of charities to siphon funds for militant operations. Those charities fell under scrutiny by security forces and more or less dried up as a funding source," said Zachary Abuza, professor at the National War College in Washington, referring to an infamous Southeast Asia-wide jihadist network.

"It is not a surprise that pro-Islamic State groups have turned to social media to make appeals for donations as Islamic State has such a slick and widespread presence across so many different social media platforms."

Indonesia has clamped down on Islamic extremism in recent months, arresting at least 160 pro-IS militants since the first attack linked to the group in January last year. At the end of October, police arrested nine suspected terrorists in East and Central Java, South Sulawesi, and Riau. In East Java, authorities arrested a man with ties to Bahrun Naim, an Indonesian militant in Syria who masterminded the 2016 Jakarta attacks that killed eight people. The man had been communicating with Naim through the messaging app Telegram, where the pair had belonged to a group called 'Kulak Tahu' (tofu seller).

Encrypted messaging platforms such as Telegram and WhatsApp are proving popular not only with active terror cells in Indonesia, but even with militants who are already behind bars. Authorities suspect the services are used by imprisoned terrorists, using mobile phones smuggled into their jails, to propagate their ideologies and even direct attacks from the comfort of their cells.

For this reason, the Indonesian communications ministry in July temporarily blocked web-access to Telegram, rescinding the order only after the company's CEO Pavel Durov pledged to help the ministry close down radical chat groups.

Meanwhile, online payment services such as PayPal and cryptocurrencies are also proving popular with the modern jihadi because they facilitate anonymous payments, according to the PPATK.

Terror funding had not entirely migrated online, the report found. It noted that wire transfers by expatriate workers in Hong Kong, Malaysia and Australia had reportedly been used by Indonesian jihadis to buy and import weapons from the southern Philippines. It said terror cells in Indonesia had received US$763,000 in foreign donations between 2014 and 2015. In one case, Dian Yulia Novi, a former migrant who worked in Singapore and Taiwan, had sent US$800 to an Indonesian terror cell. She was later arrested in Indonesia, suspected of planning a suicide attack on the presidential palace.

Return to Top

HEADLINE	**11/07 French-Swiss anti-terror sweep nets 10**
SOURCE	**http://www.reuters.com/article/us-france-security/french-arrest-nine-swiss-one-in-joint-anti-terrorism-swoop-idUSKBN1D714K?il=0**

GIST	PARIS (Reuters) - French police arrested nine people and another was arrested in Switzerland in coordinated counter-terrorism swoops that follow a spate of deadly attacks in Europe in recent years. Swiss officials said a 23-year-old Colombian woman was taken into custody after police raids there. A Swiss man aged 27 was among those arrested in parallel French police swoops linked to Islamist militant activity, they added. French police conducted simultaneous raids on premises on the eastern edge of Paris and in the southeastern region that borders Italy and Switzerland, taking nine people into custody, a source in the French judiciary said. Those arrested were aged from 18 to 65 years, said the French source, who spoke on condition of anonymity -- standard practice for most French officials on such matters. Le Parisien newspaper said it was possible the raids had thwarted an attack. The French judicial source spoke of suspected participation in a criminal terrorist network and of communications via the Telegram network that many militants use because messages can be encrypted. A Swiss statement cited suspected involvement in terrorist activity and banned Islamist militant groups such as al Qaeda and Islamic State. The arrests took place a week after France introduced tougher national security laws to permanently replace emergency powers given to police and intelligence services following deadly attacks by Islamist militants on Paris two years ago. More than 240 people have been killed in France since early 2015 in attacks by Islamist militants or assailants inspired by the Islamic State group, which has sought to establish a caliphate in Syria and Iraq and called for attacks on France. France is among countries contributing to military operations against Islamic State in Iraq and Syria. French Interior Minister Gerard Collomb, who says 32 attack plots have been thwarted in the past two years in France, played down the latest operation when asked about it during a visit to Berlin. “It’s part of operations which, sadly, are conducted relatively regularly, where we arrest a number of people we consider dangerous,” he said.
Return to Top	

HEADLINE	**11/07 Doctor denies financing NY bomb plots**
SOURCE	**http://abcnews.go.com/International/wireStory/filipino-doctor-denies-financed-york-bombing-plots-50980090?cid=clicksource_76_2_hero_headlines_headlines_hed**
GIST	A Filipino doctor accused by U.S. authorities of plotting attacks in New York City, including Times Square, appeared in a Manila court Tuesday and told reporters that money he sent to a charity was misconstrued as funds intended to finance the disrupted plots. Russell Salic smiled as he was led away in handcuffs by government agents after his brief appearance at the Manila court that is handling a U.S. extradition request, which he and his lawyer vowed to fight. "That's not true," Salic said when asked by reporters about the allegations. "I just donated money without any malicious intent." He said U.S. authorities may have mistaken the money he sent to a charity as funding for the plots. An FBI agent who posed as a Muslim online was behind the allegations against him, he said.

	A U.S. Department of Justice representative, Christopher Cardani, who attended the court hearing said the department would do everything to have Salic extradited to stand trial in America. "This is an extremely serious matter in the United States," Cardani told reporters. "It's been alleged these three individuals conspired to build a bomb and explode it at Times Square in New York in the summer of 2016 and it doesn't get any more serious than that." Last month, U.S. prosecutors said Salic was one of three Islamic State group sympathizers who plotted bombings and shootings last year at New York City concert venues, subway stations and Times Square before U.S. agents thwarted the plot. Salic was taken into custody in Manila in April. Canadian citizen Abdulrahman El Bahnasawy was arrested in the U.S. last year and has pleaded guilty, and an American of Pakistani origin, Talha Haroon, was arrested in Pakistan in November.
Return to Top	

HEADLINE	**11/07 NATO to send more troops to Afghanistan**
SOURCE	**https://www.upi.com/Top_News/World-News/2017/11/07/NATO-to-send-3000-more-troops-to-Afghanistan/5601510097631/?utm_source=fp&utm_campaign=ts&utm_medium=5**
GIST	Nov. 7 (UPI) -- NATO plans to send an additional 3,000 troops to Afghanistan to bolster the Afghan army in its fight against the Taliban, Secretary-General Jens Stoltenberg said Tuesday. Stoltenberg told reporters at a press conference in Brussels that the alliance will increase the number of troops in Afghanistan from 13,000 to 16,000 to train Afghan Special Operations Forces as part of its Resolute Support operation. "We have decided to increase the number of troops ... to help the Afghans break the stalemate, to send a message to the Taliban, to the insurgents that they will not win on the battleground," he said. The troops will not perform combat operations, but will focus on training, assisting and advising Afghan troops. "We are going to help them with developing their air force," Stoltenberg said. "The Afghans are now more and more capable of conducting air operations themselves, and we will help them with military schools, improved command and control." Stoltenberg added about half the new troops would come from the United States, while the rest would be supplied by the other 28 NATO member nations.
Return to Top	

HEADLINE	**11/07 Airstrikes on ISIS targets drop 60%**
SOURCE	**https://www.newsmax.com/newsfront/airstrikes-isis-targets-drop/2017/11/07/id/824682/**
GIST	American and coalition planes decreased the number of bombs they've dropped on Islamic State (ISIS) targets by 60 percent in October because the terror group is on the run. According to the Washington Examiner, Air Force Brig. Gen. Andrew Croft told reporters at the Pentagon that the amount of ISIS-controlled territory is on the decline. "That's indicative of the fact that ISIS is collapsing, not only as a physical caliphate but also in ownership of land," Croft said. "They only now control about 4 or 5 percent of the original area they covered, so the number of targets has dropped dramatically in the last month."

	The Examiner reported that between 1,800 and 2,600 bombs were dropped on ISIS targets in Iraq and Syria every month from January-September. In October, that figure stood at about 850. The shift is allowing the U.S. to redirect some of its efforts to Afghanistan to help that nation's government battle Taliban fighters.
Return to Top	

Suspicious, Unusual

Top of page

HEADLINE	**11/07 Pentagon: known USAF 'systemic issue'**
SOURCE	**http://www.foxnews.com/us/2017/11/07/botched-air-force-handling-texas-shooters-criminal-history-may-be-systemic-issue.html**
GIST	The Air Force's failure to report Texas church shooter Devin Kelley's domestic violence conviction to the FBI -- a misstep that left the door open for Kelley to buy weapons -- is a systemic issue in its criminal investigations unit, according to a 2015 Pentagon analysis and a former Air Force agent who spoke to Fox News. The 2015 Department of Defense Inspector General report analyzed a sample of 1,102 convictions, including felonies, handled in the military court system and found the Navy, Air Force and Marines failed to send criminal history or fingerprint data to the FBI in about 30 percent of them. The DOD study didn't determine the reasons why the reports and fingerprints never made it to the FBI. But retired Air Force officials have come out since Sunday's shooting to blast the information sharing process. "Somebody messed up," Don Christensen, a retired colonel and former chief prosecutor for the Air Force during Kelley's case, told Pro Publica. He added that providing necessary criminal information to civilian authorities was "never done well or consistently" during his 20-year career in the military justice system. "It's a combination of laziness and people being overworked," a former Air Force Office of Special Investigations agent, who wished to remain anonymous, told Fox News on Tuesday. The agent described workplaces as being revolving doors of staffers, some who would come into detachments and get handed numerous cases to deal with on top of other daily responsibilities. As a result, he said, sometimes it was "not seen as a critical task" to handle the criminal information backlog. Kelley – who killed 26 people when he opened fire at a church in Sutherland Springs on Sunday – had a domestic violence conviction the Holloman Air Force Base's OSI unit failed to enter into an FBI database used to conduct background checks on gun buyers, officials revealed Monday. But Kelley's case wasn't just a one-time error, the 2015 report and former officials suggested. Out of the 1,102 cases between 2010 and 2012 that were analyzed in the report, officials in the three branches failed to submit fingerprints to the FBI in 304 of them. Criminal history information also was missing from 334 of them. The Pentagon report also found the Air Force did not submit the fingerprints of at least 110 convicted airmen during the period between 2010 and 2012. It's not clear yet whether Kelley was one of the 110 airmen noted in that report. Kelley was found guilty in 2012 of choking and kicking his wife and striking his young stepson hard enough to fracture his skull, according to interviews and military documents. He was also accused of threatening his wife four times with a gun. Those charges were withdrawn by prosecutors after Kelley's arraignment.

	In fact, the Pentagon has known for at least two decades about failures to give military criminal history information to the FBI, according to a 1997 report from the Pentagon's inspector general. The 2015 report urged the Secretaries of the Navy and Air Force to "take prompt action" to resolve the criminal history and fingerprint issue. It also noted the military branches agreed with the recommendations but "expressed concern regarding their jurisdictional and legal authority to collect criminal history data from individuals no longer subject to the Uniform Code of Military Justice." The Air Force said Monday it "has launched a review of how the Service handled the criminal records of former Airman" Kelley, spokesperson Ann Stefanek said in a statement.
Return to Top	

HEADLINE	**11/07 Dementia now Britain's biggest killer**
SOURCE	**http://www.telegraph.co.uk/science/2017/11/07/dementia-now-britains-biggest-killer-overtaking-heart-disease/**
GIST	Dementia is now Britain's biggest killer, overtaking heart disease for first time new figures have shown. Some 70,366 people died from Alzheimer's disease and dementia last year compared to around 66,076 deaths from heart disease. In 2015 heart disease was the biggest killer with 69,785 death, while 69,182 people died from dementia. The switch is being driven by the ageing British population, combined with improvements in heart health, as more people are prescribed statins and beta blockers to cope with high cholesterol and high blood pressure. Charities have called on the government to double its annual £132 million dementia research funding over the next five years. Projections suggest that 1.2 million will be living with dementia by 2040. Hilary Evans, Chief Executive at Alzheimer's Research UK, said: "These startling figures emphasise the health crisis we face in the UK at the hands of dementia. Year-on-year, we are seeing more people conquer and survive serious health conditions like heart disease, but deaths from dementia continue to rise. "The fact that there are currently no treatments to slow or stop the diseases behind dementia brings into sharp focus the scale of the challenge and the urgency with which we must tackle it. "Dementia may be the biggest killer in the UK today, but research has the power to stop this from being the case in the future."
Return to Top	

HEADLINE	**11/07 State's first wildlife K9 officer**
SOURCE	**http://www.king5.com/tech/science/environment/wdfw-trains-rescue-dog-for-wildlife-detection/490074212**
GIST	The Washington Department of Fish and Wildlife police just finished training their first wildlife detection dog. "Benny" is an expert at finding illegally trafficked wildlife and even guns, but there was a time the black labrador's future did not look so bright. "His original owners surrendered him because he has a lot of energy and a lot of drive," explained Benny's handler, Det. Lauren Wendt.

	That energy and drive is now Benny's best asset. Detective Wendt recognized the difficulty her fellow detectives faced trying to track endangered wildlife parts in Washington. A dog would help speed the process dramatically. Wendt found Working Dogs for Conservation and California Department of Fish and Wildlife (CDFW), who worked with her to establish a plan for creating a canine program and finding a suitable canine candidate. Then, Wendt was ready to find a dog. Benny's energy seemed like the perfect fit. She says he had an incredible hunt and toy drive but almost no obedience or manners. It took 200 hours of training to get him job-ready.
Return to Top	

HEADLINE	**11/07 Pentagon known crime reporting lapses**
SOURCE	**https://www.cbsnews.com/news/pentagon-crime-reporting-lapses-20-years/**
GIST	WASHINGTON -- The Pentagon has known for at least two decades about failures to give military criminal history information to the FBI, including the type the Air Force didn't report about the accused Texas church killer who assaulted his then-wife and stepson while serving as an enlisted airman. The Air Force lapse in the Devin P. Kelley case, which is now under review by the Pentagon's inspector general, made it possible for him to buy guns before the murderous attack Sunday at a church in Sutherland Springs, Texas. Twenty-six people were killed, including multiple members of some families. About 20 other people were wounded. Rep. Mac Thornberry, the Texas Republican chairman of the House Armed Services Committee, said he was appalled at the Air Force mistake and unsatisfied by its plans to investigate the matter. "I don't believe the Air Force should be left to self-police after such tragic consequences," he said, adding that he fears the failure to report domestic violence convictions may be more widespread. Defense Secretary Jim Mattis said Tuesday he has directed the Pentagon inspector general to review circumstances of the Kelley case and "define what the problem is." At its core, the problem is that military criminal investigative organizations have too frequently, for too long, failed to comply with rules for reporting service members' criminal history data to the FBI. As recently as February 2015, the Pentagon inspector general reported that hundreds of convicted offenders' fingerprints were not submitted to the FBI's criminal history database. The report found about a 30 percent failure rate for submitting fingerprints and criminal case outcomes. It did not determine the reasons for the lapses. In February this year, the inspector general's office launched a new review to assess compliance with updated reporting requirements. A spokesman, Bruce Anderson, said that review is ongoing. The problem has persisted much longer. A February 1997 report by the Pentagon inspector general found widespread lapses. Fingerprint cards were not submitted to the FBI criminal history files in more than 80 percent of cases in the Army and Navy, and 38 percent in the Air Force. Failure to report the outcome of criminal cases was 79 percent in the Army and 50 percent in the Air Force, the report said. In the Navy, it was 94 percent.
Return to	

Top	

HEADLINE	**11/07 Mexico military abuses go 'unpunished'**
SOURCE	**http://abcnews.go.com/International/wireStory/report-rights-abuses-mexican-military-largely-unpunished-50988690?cid=clicksource_76_4_article%20roll_articleroll_hed**
GIST	The vast majority of human rights abuses allegedly committed by soldiers waging Mexico's war on drug gangs go unsolved and unpunished despite reforms letting civilian authorities investigate and prosecute such crimes, a report said Tuesday. The Washington Office on Latin America study, described as the first comprehensive analysis of military abuse investigations handled by the Attorney General's Office, found there were just 16 convictions of soldiers in the civilian judicial system out of 505 criminal investigations from 2012 through 2016, a prosecutorial success rate of 3.2 percent. Moreover, there were only two "chain of command responsibility" convictions for officers whose orders led to abuses, it said. The report said factors that hinder civilian investigations of the military include parallel civilian and military probes, limited access to troops' testimony and soldiers tampering with crime scenes or giving false testimony. "This militarized public security model has negatively impacted Mexico's criminal justice system. The civilian justice system faces challenges — including military authorities' actions resulting in the obstruction or delay of investigations — which limit civilian authorities' ability to sanction soldiers implicated in crimes and human rights violations," the group said. The Attorney General's Office, the Defense Department and other government offices did not immediately respond to requests for comment. The military has played a central role in the war on drug cartels since at least late 2006, when newly installed President Felipe Calderon deployed soldiers across the country to fight the gangs. The militarized offensive has continued under current President Enrique Pena Nieto. During that time there have been numerous accusations of serious human rights violations by soldiers, such as torture, killings and forced disappearances. Critics say the Mexican military is not trained to carry out policing activities. However, many police departments in the country are seen as corrupt, outgunned and even in cahoots with organized crime gangs, and thus unreliable allies against the cartels. Reforms in 2014 changed how allegations of abuses by the military can be investigated, including the right to conduct a civilian probe in such cases and for victims to participate. Among the 16 successful prosecutions of soldiers carried out by the Attorney General's Office are convictions for the cover-up of a human rights violation and desecration of a corpse; forced disappearance; homicide; injuries and trespassing, and rape, the report said.
Return to Top	

HEADLINE	**11/07 NASA: volcanic activity Antarctica**
SOURCE	**http://dailycaller.com/2017/11/07/nasa-has-more-evidence-volcanic-activity-is-heating-up-antarcticas-ice-sheet/**
GIST	Ancient underground streams of heated rock, called a mantle plume, might be an explanation for the instability of Antarctica's western ice sheet, according to a new NASA study.

	Scientists have been debating whether or not mantle plume heat contributes to western Antarctica's instability. Some recent studies provided evidence this might be the case, but even this study's authors were skeptical. "I thought it was crazy," Hélène Seroussi, the study's co-author and scientist at NASA's Jet Propulsion Laboratory, said in a release. "I didn't see how we could have that amount of heat and still have ice on top of it," Seroussi said in a statement. NASA says Seroussi's study provides more evidence of geothermal activity underneath a portion of the world's largest ice sheet. Scientists tend to worry more about future global warming's effect on Antarctic ice sheet. NASA glaciologist Eric Rignot said western ice sheet collapse is "unstoppable" and could dramatically raise sea levels. However, Antarctica has gone through periods of instability in the past. Seroussi's study provides important context for the western ice sheet's instability, and how mantle plumes may play a role. Seroussi's study showed a mantle plume pushes 150 milliwatts per square meter of heat up towards the ice sheet. That's about two to three times the heat flux of regions of the world without volcanic activity. A 2014 University of Texas study found western Antarctica was a literal hotbed for geothermal heat. Researchers concluded that "large areas at the base of Thwaites Glacier are actively melting in response to geothermal flux consistent with rift-associated magma migration and volcanism." The following year, another team of U.S. scientists found there's a huge amount of geothermal heat under western antarctica. "The high geothermal heat flux may help to explain why ice streams and subglacial lakes are so abundant and dynamic in this region," the study found. Earlier this year, Scottish researchers found 91 previously unidentified volcanoes under the Antarctic ice sheet, including one that's some 13,000 feet tall. If one of these volcanoes were to erupt it could further destabilise west Antarctica's ice sheets," Robert Bingham,a study co-author, told The Guardian. "Anything that causes the melting of ice – which an eruption certainly would – is likely to speed up the flow of ice into the sea. "The big question is: how active are these volcanoes? That is something we need to determine as quickly as possible," Bingham said.
Return to Top	

Crime, Criminals

Top of page

HEADLINE	**11/07 Man set on fire in north Seattle**
SOURCE	**http://www.seattlepi.com/local/crime/article/Man-set-on-fire-in-North-Seattle-12340225.php**
GIST	Seattle police are looking for two persons after a man was reportedly set on fire in North Seattle on Tuesday night. A bystander called 911 about 7 p.m. when he saw a "man on fire" in the 4500 block of Leary Way Northwest, the area between Ballard and Fremont known as "Frelard." Medics took the man to Harborview Medical Center, where he was listed in critical condition.

	Detectives now seek a man they believe set the fire and his girlfriend.
Return to Top	

HEADLINE	**11/08 Japan yakuza struggle to earn living**
SOURCE	**http://www.nippon.com/en/features/c04202/**
GIST	These are hard times for Japan's yakuza. Successive splits have divided the strength of the powerful Yamaguchi-gumi criminal gang. In the initial rupture of August 2015, a Kobe faction broke away. Then this group itself fragmented in April 2017, leaving three organizations: the Yamaguchi-gumi, Kobe Yamaguchi-gumi, and Ninkyō Yamaguchi-gumi. The primary reason for the splits is that gang members now struggle to make a living. At one time, wearing the Yamaguchi-gumi crest and leading a group of young men ready to put their lives on the line was a path to achieving the "gangster dream." Yakuza members who have completed a drinking ritual with the organization boss are known as jikisan and are considered directly subordinate to him. These jikisan once had riches to spend on houses, cars, and women. However, recent amendments to legislation and nationwide ordinances targeting organized crime have tightened the screws to the point where yakuza cannot make ends meet. Yamaguchi-gumi membership fees amount to ¥850,000 per month. Rebelling against this financial burden and rigid control by the gang leadership, the Kobe faction—centered on Inoue Kunio, leader of the Yamaken-gumi, the organization's largest group—went independent, setting fees for its jikisan at less than ¥300,000. When this loss of revenues from the broader membership pressed the new group to demand higher payments from members of its central Yamaken-gumi faction, their brewing discontent led to the formation of the breakaway Ninkyō Yamaguchi-gumi. Past Riches a Distant Dream Yakuza income has become severely constrained. Tougher legislation has made it difficult for gangs to earn money from lawful business, so they must now rely primarily on their illegal activities. The main areas are drugs and telephone scams. In the Yamaguchi-gumi, dealing drugs is ostensibly taboo, but the gang turns a blind eye to endeavors by individual members. Although the trade is highly risky, to some extent the group's survival depends on the high returns gained from methamphetamine sales. Scamming elderly members of the public also falls considerably short of the image of chivalry that the yakuza like to project, but the business continues regardless. There are still some legitimate fields, like real estate and finance, that provide room for the gangs' dirty work. It can be useful for businesses trying to navigate complex property rights issues, for instance, to have a muscle backing. Jobs like this remain in Tokyo in particular. Criminal organizations can also profit from trading when a listed company hits an economic slump. Meanwhile, new areas like online peer-to-peer lending and cryptocurrency are prime environments for yakuza fraud. However, this kind of business is just a tenth or a twentieth of the scale it was in Japanese crime's bubble-era heyday. The reason for the change is clear. Until the bubble era, yakuza groups made money both legally and illegally, but the government's tightened restrictions and beefed-up compliance have frozen gangs out of corporate earnings. Now they must rely primarily on illicit business. Typical legal business fields for yakuza involvement included finance, real estate, construction, entertainment, staffing, demolition, industrial waste, liquidation of companies, debt collection, and settling disputes within their territory. Illegal areas included gambling, drugs, prostitution, telephone fraud, protection rackets, and impersonating lawyers. If they relied only on legal business, gangs would be much like ordinary companies, but it was hard to

	walk away from the boosted earnings made possible by a combination of activities inside and outside the law. Affiliated financial operatives could ignore legal upper limits on interest rates and make highly risky loans to companies in the certain knowledge that they would get their money back. At the time, some viewed the yakuza as a necessary evil to some extent, performing activities that were of some value to legitimate society. In the financial sphere, for example, they could supply money at short notice when it was really needed, while in the real estate industry they were able to acquire land by all available means within a given time limit. They could deliver workers for dangerous jobs and ensure that debts could be recovered even when the claimant was competing with other creditors. They were generally tolerated, at least until the first of several antigang laws came into force in 1992. The Act on Prevention of Unjust Acts by Organized Crime Group Members came into force in 1992. The government intensified its attack with numerous follow-up amendments. An expanded interpretation of conspiracy connected underlings' crimes to the kumichō, who also became a target for damages under civil law. The yakuza's vaunted pyramid structure began to crumble. By 2005, when Tsukasa Shinobu rose to leadership, the gang was putting an ever-greater emphasis on not doing anything that would harm the kumichō. At the same time, jikisan were enduring the squeeze of higher tribute payments. Local ordinances drove a wedge between gangsters and their civilian collaborators by legally considering anyone who associated with the yakuza to themselves be "antisocial forces." By October 2011, this sort of legislation was active in all 47 of Japan's prefectures. Celebrity Shimada Shinsuke was forced to retire from show business in August of the same year because of his ties to organized crime. The offering up of this popular TV star as a sacrifice sent a powerful message to society. Gang members were not allowed to have bank accounts or rent property, and were effectively deprived of their rights to make a living. Yakuza organizations are now getting by with drastically reduced income. Despite their swaggering front, they risk complete collapse. And nobody knows that better than the gangsters themselves.
Return to Top	

HEADLINE	**11/07 Claim: gunman deliberately shot babies**
SOURCE	**http://www.foxnews.com/us/2017/11/07/air-force-admits-fault-in-reporting-shooters-past-crimes.html**
GIST	SUTHERLAND SPRINGS, Texas – The gunman who killed 26 people at a small-town Texas church went aisle to aisle looking for victims and shot crying babies at point-blank range, a couple who survived the attack said. Rosanne Solis and Joaquin Ramirez were sitting near the entrance to the First Baptist Church on Sunday when they heard what sounded like firecrackers and realized someone was shooting at the tiny wood-frame building. In an interview with San Antonio television station KSAT, Solis said congregants began screaming and dropped to the floor. She could see bullets flying into the carpet and fellow worshippers falling down, bloodied, after getting hit. For a moment, the attacked seemed to stop, and worshippers thought that police had arrived to confront the gunman. But then he entered the church and resumed "shooting hard" at helpless families, Solis said. The gunman checked each aisle for more victims, including babies who cried out amid the noise and smoke, Ramirez said. The couple survived by huddling close to the ground and playing dead. Solis was shot in the arm. Ramirez was hit by shrapnel. About 20 other people were wounded. At least five were still hospitalized Tuesday.

Return to Top

HEADLINE	11/07 Penn. trooper shot during traffic stop
SOURCE	http://www.foxnews.com/us/2017/11/07/pennsylvania-state-police-trooper-shot-during-traffic-stop.html
GIST	NAZARETH, Pa. – A Pennsylvania State Police trooper has been shot during a traffic stop, and a suspect is believed to be in custody. State police say the trooper was shot Tuesday on state Route 191 in Plainfield Township, Northampton County, about 65 miles north of Philadelphia. The trooper's condition was not immediately known. Citing emergency radio reports, local media reported the suspect is in custody at Easton Hospital. Asked to confirm, Northampton County District Attorney John Morganelli told The Associated Press, "I believe that to be the case." There's a heavy police presence at the hospital. A car with its back window shot out that matches the description of the suspect's car is in the parking lot, marked with police tape. Gov. Tom Wolf tweeted that he is "praying for this trooper and their family."
Return to Top	

HEADLINE	11/07 Strangers acted together to stop shooter
SOURCE	http://www.cnn.com/2017/11/07/us/church-shooting-heroes-reunite-trnd/index.html
GIST	(CNN)On that awful Sunday morning, they were just strangers, trying to stop an act of unspeakable evil. On Monday night, they reunited as heroes, hailed for the actions they took that helped end the deadliest mass shooting in Texas history. Stephen Willeford and Johnnie Langendorff hugged each other at a vigil held for the 26 killed and more than 20 wounded in the shooting at First Baptist Church in Sutherland Springs. When Devin Patrick Kelley opened fire inside the church on Sunday, Stephen Willeford, who lives near the church, grabbed his own gun and ran out of the house barefoot to confront the gunman. "I kept hearing the shots, one after another, very rapid shots - just 'pop pop pop pop' and I knew every one of those shots represented someone, that it was aimed at someone, that they weren't just random shots," Willeford told CNN affiliate KHBS. Willeford exchanged gunfire with Kelley as started his escape in his Ford Explorer. He spotted Johnnie Langendorff's truck across the street and hailed him down. "I said, 'that guy just shot up the Baptist church. We need to stop him," Willeford told the affiliate. Langendorff didn't hesitate. "I had to make sure he was caught," Langendorff told CNN. "It was, 'Do everything necessary to make sure that this guy is stopped.'" The men pursued the gunman for 11 miles, in a chase that reached speeds of 95 mph. Kelley eventually lost control of his truck and crashed it in a ditch. Police found him dead, with gunshot

	wounds, one of them self-inflicted. Langendorff said he had no regrets about throwing himself into such a dangerous situation. "Because that's what you do, you chase a bad guy," he said. Willeford wished he could have gotten to the church faster to stop Kelley. He doesn't consider himself a hero, but the county's sheriff disagrees. "What do you say to the man who stepped up when he heard the gunshots? I'd say he's a hero," Wilson County Sheriff Joe Tackitt Jr. said. "I don't think there's any question about that. Had he not done what he did, we could have lost more people."
Return to Top	

HEADLINE	**11/07 Assault rifle role in mass shootings**
SOURCE	**http://abcnews.go.com/US/assault-rifles-played-prominent-role-us-mass-shootings/story?id=50962470&cid=clicksource_4380645_1_hero_headlines_bsq_hed**
GIST	Americans are grappling with yet another massacre after a Texas church's Sunday morning services were interrupted by a masked gunman who sprayed parishioners with bullets shot from an AR-15 platform rifle. Former Air Force veteran Devin Kelley killed 26 people -- many of them children -- and also left 20 people injured in what authorities have called a "domestic situation." The murder weapon he used, authorities said, is the AR-15 assault rifle, which is popular with hunters. The AR-15 rifle and similar makes are favored by shooters for their magazine-fed, gas-operated semi-automatic action. These rifles can also be customized. The initials “AR” stands for ArmaLite Rifle, not to be misconstrued as “Assault Rifle” or "Automatic Rifle," based on the original AR-15 invented by American engineer Eugene Stoner of ArmaLite Inc. in the late 1950s. From its inception, the AR-15 became known as a weapon prized for being lightweight, accurate and able to fire multiple rounds. The AR-15 isn't subject to the National Firearms Act, a law passed in 1934 that bans the possession of machine guns by civilians. What's more, Ronald Turk, associate deputy director and chief operating officer of The Bureau of Alcohol, Tobacco, Firearms and Explosives (ATF), released a report this year inadvertently loosening the stigma on AR-15s by referring to them as "“modern sporting rifles.” "These firearm types are now standard for hunting activities," Turk wrote. He acknowledged, however, that hunting is "vastly different than what it was years ago" and there should be a "reissue" of the 20-year-old "New Sporting Purpose" study to "re-examine" safety interests. These results should be made public to "address any concerns," he argued. According to a National Rifle Association blog post titled “Why the AR-15 is America's Most Popular Rifle,” the weapon's design was mimicked to create the automatic M-16 rifle, which is issued and still used today by American soldiers. But the AR-15 has also been likened to “weapons of war” by President Obama in the wake of the Pulse Nightclub shooting in Orlando, Florida, where 29-year-old Omar Mateen slaughtered 49 and wounded 53 people in June 2016.

And it’s the same rifle that keeps reappearing again and again as a murder weapon in mass shootings.

These are the five most recent AR-15-involved mass shootings in the U.S.

Las Vegas, Nevada: 58 people and injured over 500 people killed on Oct. 1, 2017

Perched from his two-room hotel suite at the Mandalay Bay Resort and Casino, Stephen Paddock, a 64-year-old retiree and avid video poker gambler, fired on hundreds of country music fans attending an outdoor country music festival.

The killer checked in on Sept. 28 with 10 bags and at least 23 guns, including AR-15-style and AK-47-style rifles and a "large cache of ammunition."

Some of rifles were rigged with bump stocks, kits that mimic the firing of an automatic machine gun.

Paddock set up surveillance cameras inside and outside his suite but ultimately committed suicide, authorities said, when SWAT teams responded to his room.

Orlando, Florida: 49 people killed, 53 wounded on June 12, 2016

In the early morning of June 12, 2016, 29-year old Omar Mateen crashed a night of partying at Pulse, a gay nightclub, in Orlando, Florida, and killed 49 people and injured 53 others.

Mateen took clubgoers hostage before slaying them. He died after engaging in a firefight with authorities.

The massacre was staged with an AR-15-style rifle and a handgun from a federally licensed dealer near Mateen's home in Fort Pierce, Florida.

San Bernardino, California: 14 people killed, 22 people wounded on Dec. 2, 2015

Syed Rizwan Farook and his wife, Tashfeen Malik, stormed the Inland Regional Center during a Department of Public Health training session and holiday party to shoot and kill San Bernardino county workers assembling together.

Farook was an employee with the division and worked alongside many of the victims for years. According to the FBI, he used two semi-automatic AR-15 rifles in his attack.

After the killing spree, Farook and Malik were killed by police as they tried to make a getaway.

Colorado Springs, Colorado: 3 people killed on Oct. 31, 2015

That Halloween morning, Noah Harpham, 33, armed with an AR-15 rifle, a 9 mm pistol and a .357 revolver killed a bicyclist and two women before being shot by police.

Witnesses reported Harpham walking down a street carrying a rifle and two gas cans.

Chattanooga, Tennessee: 4 people killed, 3 people wounded on July 16, 2015

Mohammod Youssuf Abdulazeez shot and killed four Marines and wounded three other people when the 24-year-old opened fire on the Naval Operation Support Center and an Armed Forces Recruiting Center.

Abdulazeez, of Hixson, Tennessee, was killed in a firefight with responding police officers after the rampage.

Investigators said the University of Tennessee-Chattanooga graduate possessed a Kalashnikov variant

	rifle, a Smith & Wesson handgun and a Saiga-12 semiautomatic shotgun. An AR-15 semiautomatic assault rifle was pulled by investigators from his family's home.
Return to Top	

HEADLINE	**11/07 Ohio busts 100 in fentanyl drug ring**
SOURCE	**http://www.cleveland.com/metro/index.ssf/2017/11/cleveland-based_gang_members_a.html#incart_river_home_pop**
GIST	CLEVELAND, Ohio -- Three men who investigators identified as members of the Cleveland-based "Down the Way" street gang led a 100-member drug dealing ring that trafficked enough heroin, fentanyl and cocaine to kill everyone in 12 counties in southeastern Ohio, authorities said. Ohio Attorney General Mike DeWine and Columbiana County law enforcement officials on Tuesday announced a 756-count indictment against 100 people accused of trafficking heroin, fentanyl, carfentanil and cocaine from Cleveland to small towns along the Ohio River, including East Liverpool. Two of the accused ringleaders -- Tremaine Jackson, 28, of Cleveland, and Jermaine Jackson, 46, of Garfield Heights -- were among 24 people taken into custody by Tuesday afternoon. DeWine's office did not release the names of the other 76 people charged in the indictment filed in Columbiana County Common Pleas Court. The group funneled about 1 million doses of carfentanil and approximately 350,000 doses of fentanyl into Columbiana County, enough to kill every person in that county and 11 surrounding counties, DeWine's office said.
Return to Top	

HEADLINE	**11/07 Domestic violence, mass killings link?**
SOURCE	**https://www.cbsnews.com/news/link-between-domestic-violence-mass-killings/**
GIST	On Sunday, 26-year-old Devin Patrick Kelley walked into First Baptist Church in Sutherland Springs, Texas and opened fire, killing 26 people and wounding 20 others in what Texas Gov. Greg Abbott called the deadliest mass shooting in his state's history. In the wake of this tragedy – as is often the case after similar attacks – many are left asking why and how could it happen. While there is no easy answer, investigators have seen a common thread in more than half of the spate of mass shootings in the U.S. in recent years: domestic violence. In fact, a recent analysis of FBI data by the group Everytown for Gun Safety found that over a five-year period, 54 percent of mass shootings were related to domestic or family violence and included the killing of a partner or other family member. Kelley had a history of domestic violence. U.S. Air Force records show he was court-martialed in 2012 for assaulting his then-wife and young stepson, fracturing the child's skull. He was convicted and received a one-year sentence. A 2012 police report obtained Tuesday revealed that Kelley had escaped from a behavioral health center where he had been sent while facing charges for the assaults. In the report, he was described as "a danger to himself and others" who was "attempting to carry out death threats that [he] had made on his military chain of command." Mary Ellen O'Toole, former FBI profiler and director of the forensic science program at George Mason

University notes that although domestic violence is not a predictor for mass shootings, there appears to be some connection.

"There are many people who do engage in domestic violence and never go on to become mass killers, but because it's prominent in a number of cases we've seen over time, it really does need to be considered as perhaps one of the warning behaviors that we already know about," O'Toole told "CBS This Morning."

After the 2012 case, Kelley got divorced and married a second time. According to Texas investigators, at the time of the church shooting "there was a domestic situation going on" involving Kelley and his in-laws. He had reportedly sent threatening texts to his mother-in-law, who attended the church, though she was not there at the time of the shooting.

But O'Toole said that Kelley's violent intentions clearly extended far beyond a desire to confront his mother-in-law.

"He was really mission-oriented. His intent was maximum lethality," she said. "When someone is intent on maximum lethality because they want to kill as many people as they can, engaging in that behavior makes them feel powerful, it makes them feel omnipotent, it underscores their predatory behavior so they're intent was far beyond just killing a single person."

Lori Post, a violence researcher and director of the Institute for Public Health and Medicine Buehler Center for Health Policy and Economics at Northwestern University, noted a number of signs that the rampage was premeditated.

"He planned and organized this and knew exactly what he was going to do. He had to investigate the church time, transportation to and from the massacre, weapons and ammunition," she said.

Post put it bluntly: "Everything we know about domestic violence predicted this could happen."

Texas and federal laws prohibit those with domestic violence convictions from owning firearm, although there are some loopholes. The military is supposed to report to the FBI convictions on domestic violence charges, as well as convictions that carry maximum potential sentences of more than a year in confinement, so that perpetrators can be put in a federal database and denied gun purchases. However, the U.S. Air Force admitted Monday it failed to do so in Kelley's case.

A history of domestic violence is a pattern seen in other mass shootings as well. In September, 32-year-old Spencer James Hight shot and killed eight people at a football party in Plano, Texas, including his 27-year-old estranged wife, Meredith Emily Hight. According to Meredith Hight's mother, Debbie Lane, her daughter was seeking a divorce because Spencer was an alcoholic and was physically abusive.

"After two years of trying to get him in treatment, trying to get him to stop, trying to help him… she said, enough is enough. She made every effort she could… and could leave that relationship with no regrets," Lane told CBS DFW.

Plano Police Chief Greg W. Rushin called the crime the worst mass shooting in the city's history.

"We've never had a shooting of this magnitude; never had this many victims," he said.

In Kelley's case, there was also another troubling sign in his past: animal abuse.

The Denver Post reports he was cited for misdemeanor animal cruelty in 2014 while living in a mobile home park near Colorado Springs. Numerous witnesses told police they saw him beat a dog with his fists.

O'Toole said there are other warning signs that someone may be getting ready to commit a mass killing.

"Some of those include things like leakage. That means that someone tells a person either directly or

	indirectly what they're going to do," she said. Behavioral changes are also often seen, including becoming obsessed with other mass killers, amassing more firearms, or going out and practicing shooting.
Return to Top	

HEADLINE	**11/07 Air Force: Tex. shooter 'serious problem'**
SOURCE	**https://www.cbsnews.com/news/air-force-secretary-says-texas-shooter-was-a-serious-problem-in-the-air-force/**
GIST	Air Force Secretary Heather Wilson says Texas gunman Devin Kelley was "clearly a serious problem" in the Air Force, evident from the fact that he was court-martialed for assaulting his then-wife and small stepson. Wilson, in a Tuesday interview with CBSN, would not directly say whether the Air Force suspected Kelley posed a threat to others in his time with the service. Kelley, who joined the Air Force after graduating high school in 2009, was court-martialed in 2012 and convicted for assaulting his then-wife and his stepson. He was confined for a year, and given a bad conduct discharge. On Sunday, Kelley entered First Baptist Church in Sutherland Springs, Texas, and gunned down dozens of worshipers, killing 26 people as young as 18 months old. "I've got to be a bit careful about the records I've seen," Wilson told CBSN. But Wilson did acknowledge Kelley was "clearly a serious problem in the Air Force," mentioning his assault conviction. An office within the Air Force failed to place Kelley's conviction in a federal database, which would have shown up in his background check and likely prevented him from legally purchasing firearms. Asked how the Air Force let that fall through the cracks, Wilson pointed to the review the Pentagon's inspector general is conducting. "Well, that's why we have initiated the review of this case and all others like it, is to find out those facts," Wilson told CBSN. Wilson said it's "pretty clear that the check list we use was not followed by the local office" in New Mexico, and his fingerprints "should have been" in the database, when they were not. The Air Force is under fire for its failure to properly report Kelley's assault conviction, with members of Congress and the public questioning how Kelley's conviction went unnoticed in federal records, and whether such reporting failures are systemic. On Tuesday, an exasperated Speaker of the House Paul Ryan, R-Wisconsin, wondered aloud how Kelley slipped through the cracks of the system. "This speaks to making sure we actually enforce our laws that we have on the books," Ryan said.
Return to Top	

HEADLINE	**11/08 China: UCLA basketball players arrested**
SOURCE	**http://abcnews.go.com/Sports/ucla-basketball-players-arrested-china-shoplifting-charges/story?id=50994342&cid=clicksource_4380645_1_hero_headlines_headlines_hed**
GIST	Three freshmen UCLA basketball players have been arrested in China on shoplifting charges, ESPN reported. Among the arrested was LiAngelo Ball, younger brother of Los Angeles Lakers point guard Lonzo Ball, a source told ESPN. Cody Riley and Jalen Hill were also arrested, according to ESPN.

	The UCLA basketball team is in China to play its season opener against Georgia Tech in Shanghai. ESPN reports the players were being questioned about stealing from a Louis Vuitton store located next to the team's hotel in Hangzhou. "I am not quite clear about the specific information," Chinese Foreign Ministry spokeswoman Hua Chunying said in a briefing Wednesday. "The Chinese side has already informed the U.S. side of the relevant case in accordance with the consular treaty between the two sides. China will handle this case in accordance to the law and ensure the legitimate rights of the persons involved." Around 8 a.m. Tuesday, about 20 police officers went to the Hyatt in Hangzhou to speak to several players from both teams, a source told ESPN. The players were not allowed to speak to any coaches as they were kept in a room for hours, ESPN reported. The Georgia Tech players were later allowed to leave the room, but the UCLA players were seen getting into a police vehicle around 1 p.m., according to ESPN.
Return to Top	

HEADLINE	**11/07 Shooter escaped mental facility 2012**
SOURCE	**http://abcnews.go.com/US/texas-shooting-suspect-escaped-behavioral-center-2012-attempted/story?id=50985821**
GIST	Texas church shooting suspect and Air Force veteran Devin Kelley escaped from a New Mexico mental health hospital in 2012, according to an El Paso Police Department report, which also said he "was attempting to carry out death threats" that he "had made on his military chain of command." A witness said Kelley "suffered from mental disorders and had plans to run from Peak Behavioral Health Services ... and take a bus out of state," according to the report. The report said Kelley had previously been caught sneaking firearms onto Hollaman Air Force Base where he served in New Mexico. The report also noted that Kelley was facing military criminal charges. Kelley was located and did not resist or make any comments about harming himself or other officers, the report said, adding that he was released to Sunland Park police officers. The Air Force official confirmed the details in the police report, including that Kelley was a danger to himself and others, faced military criminal charges, had been sneaking firearms onto Holloman Air Force Base and had made threats toward his chain of command. The official also confirmed the description from the person at the facility that Kelley "suffered from mental disorders." Peak Behavioral Health said in a statement today, "We are deeply committed to providing the best patient care. We never discuss whether someone was or was not a patient at our hospital, and we never discuss any information about our patients. Preserving the confidentiality of this information is not only a matter of policy, it is federal and state law." The facility added, "Our hearts go out to the victims of this horrible act and their families and friends, and like everyone else in Texas, we are doing everything we can to help the community in recovering and healing from this tragedy."
Return to Top	

HEADLINE	**11/07 Latest on Texas church shooting**
SOURCE	**http://www.cnn.com/2017/11/07/us/texas-church-shooting/index.html**

GIST	(CNN)Devin Patrick Kelley had previously attended the small Texas church where he killed 26 people over the weekend but he was not welcomed there, Wilson County Sheriff Joe Tackitt told CNN Tuesday. The pastor of First Baptist Church, Frank Pomeroy, knew Kelley from his attendance at church events, according to Tackitt. The pastor wanted him out. There were no threats but Pomeroy told authorities Kelley "was not a good person to be around." "He did not think that he was a good person and did not want him around his church," Tackitt said of the pastor. "But he said, 'How do I run him away from my church?'" On Sunday, Kelley reappeared at the church. This time, he was armed with an assault rifle, 15 loaded magazines and an obsession with a family dispute. As investigators try to piece together a picture of Kelley, more clues have emerged in the deadliest shooting in modern Texas history. The dead parishioners from the First Baptist Church in Sutherland Springs ranged in age from 17 months to 77 years old, and included an unborn child. Kelley, who had a record of violence, was consumed by a dispute with his mother-in-law and spent time posting anti-God and pro-gun statements on Facebook in the months before the shooting, according to officials, as well as acquaintances and former classmates. He sent threatening text messages to his mother-in-law and texted her as recently as Sunday morning -- not long before he sprayed bullets at the people in the church with an assault rifle, authorities said. He may have thought she was at church on Sunday, according to Tackitt. "There are many ways that he could have taken care of the mother-in-law without coming with 15 loaded magazines and an assault rifle to a church," said Freeman Martin of the Texas Department of Public Safety. "I think he came here with a purpose and a mission." **Latest developments** • Kelley escaped from Peak Behavioral Health Systems in New Mexico in June 2012, months after being accused of abusing his ex-wife and her child, according to documents from the El Paso Police Department obtained by CNN affiliate KVIA. • The FBI now has the shooter's cellphone, but has not yet accessed its content due to encryption, a growing challenge for law enforcement, Christopher Combs, FBI special agent in charge, said at a Tuesday news conference. • As of Tuesday, 10 of the wounded remained in critical condition, Martin said. • In an October 29 Facebook post, Kelley posted a photo of a Ruger AR-556 rifle -- the same type used in the shooting -- on a white couch, former classmates and members of the community told CNN. The caption read, "She's a bad bitch." It's not clear if it was the same weapon he used on Sunday. • The US Air Force acknowledged it did not relay information about Kelley's court martial conviction for domestic assault to civilian law enforcement, something that could have prevented him from purchasing the firearms used in the shooting. The Air Force and Department of Defense are investigating how records of his domestic violence conviction were handled. • Kelley, 26, had three gunshot wounds. He was shot in the leg and torso by an armed citizen, and had a self-inflicted shot to the head, authorities said. It wasn't clear which gunshot killed Kelley, but there was evidence at the scene "that indicates the subject may have died from a self-inflicted gunshot wound," Martin said. He was found dead in his vehicle. • Investigators have reviewed video footage from inside the church, Martin said. • Kelley was denied a license to carry a gun in Texas, Gov. Greg Abbott said. But he passed a background check required for the purchase he made in April 2016 of the Ruger AR-556 rifle he is believed to have used in the shooting.
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