Washington State Fusion Center
INFOCUS
FRIDAY – 27 APR 2018

	International	National	Regional and Local
Events, Opportunities Go to articles	04/27 India security operation targets Maoists 04/27 China, India leaders meet amid tensions 04/27 Koreas agree: end war, denuclearize 04/27 Koreas leaders in diplomatic dance 04/26 NKorea Kim crosses DMZ line 04/26 Israel warns will strike back if attacked 04/26 Israel denies killing scientist in Malaysia 04/26 UN: 10 aid workers missing South Sudan 04/26 Toronto hospital 'calm, organized chaos' 04/26 Across Europe, Jewish safety fears grow 04/26 Tourism still strong in Mexico resort areas	04/27 US, Israel heat up rhetoric on Iran 04/27 Experts: US unprepared for biothreats 04/27 Authorities: Wisconsin refinery fire out 04/27 Arizona, Colorado teachers 2nd day rally 04/27 Feds: lost track of immigrant children 04/26 Officials: MS-13 'gaming' immigration 04/26 DHS ends protected status for Nepal 04/26 More children being diagnosed autism 04/26 Parkland deputies 'no confidence' sheriff 04/26 Army accepts recruits w/behavior issues 04/25 Active shooter scare at Fort Bragg 04/24 Lessons learned from Las Vegas shooting	04/26 Seattle's Fire Station 5 reopens 04/26 Homebuyers looking outside Seattle 04/26 Homeless camp Green Lake to move 04/26 Norovirus closes Tacoma restaurant 04/26 'Breathtaking potential implications' suit 04/26 Seattle disaster drill 'power out, no bars' 04/26 DOL: 100+ salons health, safety violations 04/24 Banner year for Seattle, King Co. tourism
Cyber Awareness Go to articles	04/27 State-sponsored hacks on Australia rise 04/27 Bitcoin frenzy settles down 04/26 Dutch police shutter Anon-IB 04/26 Insider breach costs over $8.7M 04/26 NKorea elites ditching Facebook 04/26 New phishing attack uses online quiz 04/26 MongoDB server exposes Bezop users 04/26 Report: China seizes 600 bitcoin miners 04/26 Facebook criticized for 'love jihad' posts 04/25 Thailand seizes 'Hidden Cobra' servers 04/25 Majority online banking systems w/flaws	04/27 Chrome VPN extensions leaking data 04/27 World's largest spam botnet gets update 04/26 Hackers love healthcare 04/26 Crypto crime wave is here 04/26 Sounds of DDoS in NetFlow logs 04/26 Report: tech supply chain vulnerable 04/26 For sale: next-generation phishing kit 04/26 Study: non-malware attacks on the rise 04/26 Malware of mass destruction next WMD? 04/26 Phishing campaign delivers new malware 04/26 New 'interesting' C# ransomware emerges 04/26 Mass. school district pays $10,000 ransom	
Terror Conditions Go to articles	04/27 ISIS propaganda websites targeted 04/27 Turkey detains 4 senior ISIS militants 04/26 World Cup 2018 terror warning 04/26 Challenge: tracking terror financing 04/26 Afghan official: Taliban killed 7 soldiers 04/26 Arrested woman had USB w/police info 04/26 Italy detains asylum seeker in terror plot	04/27 Confronting terrorism online 04/27 Military judge rules in landmark decision 04/26 US stepping up operations against ISIS 04/26 Study: more 9/11 cancer burden cases	
Suspicious, Unusual Go to articles	04/27 Cars in Europe call police accidentally 04/26 Russia chided for 'obscene masquerade' 04/26 Rwanda official: mass graves discovered 04/25 Arctic ice w/record amount of plastic	04/27 Surging ranks of super-commuters 04/27 Iconic pen made by blind for military 04/26 JFK documents: Oswald's KGB handler 04/26 New US 24-hr precipitation record set? 04/26 Dark chocolate gives brain a boost?	04/26 Seattle ties high-record temp for day
Crime, Criminals Go to articles	04/27 Bosnia detains 12 suspicion of war crimes 04/27 Pakistan first conviction for child porn 04/26 Violent rivals rush into FARC void 04/26 Latin America amidst murder crisis 04/26 German nurse faces 98 murder charges 04/25 Vehicle rental agencies safety concerns	04/27 Privacy fears over 'genetic informants' 04/26 Bill Cosby found guilty all charges 04/26 Texas church shooter promised judge 04/26 DNA from genealogy site aided capture 04/26 Suspected serial killer shocked by arrest 04/26 Inmate bought a mail bomb off dark web 04/26 Charges dropped: teen 'planned' shooting 04/26 Virginia top court curtails police ALPR use 04/26 Police: explosive device Texas Starbucks	04/27 Hit-and-run crashes rise locally 04/27 Renton child luring suspect arrested 04/26 Everett mayor, PD chief eye gang violence 04/26 Ferry terminals: cut in line, get a fine 04/26 FBI campaign: sex assault on planes 04/26 State working thru rape kit backlog 04/26 Rape kit backlog blamed in assault

DISCLAIMER and FAIR USE Notice

Event Calendar

Top of page

Date	Event	Location/Time	Other Information

Return to Top	**indicates new event/new information added during reporting week

Events, Opportunities

Top of page

HEADLINE	04/26 Seattle's Fire Station 5 reopens
SOURCE	https://www.seattletimes.com/seattle-news/seattles-biggest-fireboat-is-back-at-its-dock-as-fire-station-5-reopens/
GIST	You may have caught a glimpse of Seattle's largest fireboat, the 108-foot Leschi, when it shoots its water cannons during spring and summer drills on Elliott Bay. Or you may have seen it during public events such as Opening Day of boating season, which is coming up May 5. To see it up close while it's docked, you can now find the Leschi at Fire Station 5 on the west end of Madison Street, right between Colman Dock and the legendary Ivar's Fish and Chips Restaurant — look for the outdoor walkway where people are having lunch and feeding the seagulls. The historic waterfront fire station closed for the seawall construction and seismic upgrades in 2014 and just reopened this week.
Return to Top	

HEADLINE	04/26 Tourism still strong Mexico resort areas
SOURCE	https://www.nytimes.com/2018/04/27/travel/mexico-tourism-violence.html
GIST	Travel operators bill Cancún and the adjoining Riviera Maya on Mexico's Caribbean coast as carefree beach escapes with something for everyone from spring break partyers to families. But a wave of violence, linked to rival drug gangs, threatens travel in the region like a storm hovering on the horizon. The local news site Noticaribe reported 14 murders in Cancún over a 36-hour period in early April, continuing a pattern of violence reported last summer. Gun deaths have also occurred in Playa del Carmen, the biggest town on the Riviera Maya, about 40 miles south of Cancún. Travelers have not been targeted in these crimes, but a bomb that detonated in February on a ferry linking Playa del Carmen with the island of Cozumel, a popular cruise port, injured more than two dozen passengers, including tourists. It prompted the Department of State to issue a travel ban on the ferry route for government employees. Reuters later reported the bomb was a homemade device believed to be unrelated to terrorists or organized crime. Since then, Mexican authorities have strengthened security around the ferry as well as the ferries that run between Cancún and Isla Mujeres, including adding metal detectors and bomb-sniffing dogs. The American government subsequently dropped its ban on ferry travel. The State Department's advisory level remains at the second of four cautionary categories, indicating travelers should "exercise increased caution." It is the same threat level of Antarctica, Denmark, Italy and Britain. Its report, updated on March 16, on the state of Quintana Roo, home to Cancún and the Riviera Maya, notes the uptick in homicides but does not restrict travel for U.S. government employees. "While most of these homicides appeared to be targeted, criminal organization assassinations, turf battles between criminal groups have resulted in violent crime in areas frequented by U.S. citizens. Shooting incidents injuring or killing bystanders have occurred," the advisory stated. Tourism authorities have responded by stepping up security. The Mexican navy patrols the beaches, federal police monitor the highways and the army is in charge of entry points into the region's cities. Dario Flota Ocampo, the director of the Quintana Room Tourism Board, said that 3,000 new surveillance cameras are being installed in the Cancún and Playa del Carmen areas. "Tourism is the main industry for the state of Quintana Roo, which is why our main concern is to provide

	security and ensure travelers have great experience because we want them to come back," Mr. Flota Ocampo said. Some 16.9 million visitors came to the state in 2017, an increase of 5.3 percent over the year prior, according to the state tourism board. Over 52 percent of those arrivals were repeat visitors. Told to exercise caution, Americans have continued to travel to the Yucatán. Whether it was the very cold winter endured in the northern United States, or the number of deals coming from the rapidly growing destination (some 14,000 hotel rooms are currently in development), tourism has shown resiliency. In the first quarter of 2018, hotel occupancy in Cancún stayed level with 2017 figures at a healthy 77 percent, even though the room inventory grew this year by 3 percent this year, according to STR, Inc., a travel research company that tracks hotel data. Travel agencies report strong interest in the region. AAA Travel predicted that Cancún would be its most popular international destination for family travelers this year. The deal site Travelzoo currently has packages at a luxury resort in Playa del Carmen at $529 for three nights for two people, just over half off. The site's senior editor, Gabe Saglie, said hotel promotions have "created some amazing value south of the border, enough to get many travelers, while cognizant of security concerns and undoubtedly traveling with heightened self-awareness and vigilance, to pounce." Bookings are up 12 percent to Mexico over this time last year at the luxury-focused travel agency Ovation Vacations in New York, even though advisers are fielding more inquiries regarding safety. "There's a lot of hesitancy, but there's resiliency," said Jack Ezon, the owner of the agency.
Return to Top	

HEADLINE	**04/26 Seattle disaster drill 'Power Out, No Bars'**
SOURCE	**http://westseattleblog.com/2018/04/saturday-citywide-disaster-drill-including-three-west-seattle-hubs-and-you-can-help/**
GIST	From Pigeon Point to High Point to Fauntleroy, three local Emergency Communication Hubs will be participating in a drill this Saturday morning, 8:30-noon – to prepare for something everyone hopes will never happen. And you can help! We've mentioned it a few times before, and here's the official announcement: Imagine there is a major power blackout covering Seattle and the metro area. There is no cellular phone service. No one knows the cause of the outage or knows when power and cell service may be restored. Emergency generators at hospitals and other essential service providers can only last as long as there is fuel. How would the region communicate? This is the scenario behind the "Power Out, No Bars" exercise that Seattle ham radio operators and designated emergency Hub volunteers throughout the City will be testing. The Seattle Auxiliary Communications Service (ACS), a volunteer organization operating under the auspices of the Seattle Office of Emergency Management, and the Seattle Emergency Communication Hubs, a grass-roots, neighborhood network of community members, will jointly conduct the citywide communications exercise. The drill simulates the day after an unexplained failure of grid power and cellular service, with no updates on when either would be restored. Because the Hubs are the major residential and business resources for neighborhoods, situational awareness, resource coordination, and communications between the Hubs, ACS, and the city's Emergency Operations Center (EOC) are critical.

	The key goals of the exercise are: *Activate several neighborhood Communication Hubs and Seattle ACS, emphasizing reliable, efficient, accurate message management and documentation. Exercise participants will use voice as well as data communications via radio, throughout the city. *Demonstrate, practice, and assess the ability to communicate up and down the various levels of the response structure, based on the Incident Command System (ICS), which spells out a hierarchical, yet flexible, means of managing emergency situations. *Build strong working relationships among Emergency Communication Hub members and ACS members, through team problem solving and practice. Exercise Scenario In an event such as the one this exercise portrays, the neighborhood Hubs would mobilize to assist with the immediate needs of residents, especially those who may need emergency services. The ACS would also have activated shortly after the scope of the outage was known, with sector sites around the city providing situation reports and helping coordinate emergency and logistical responses. “In a citywide or regional event, people will need to go to neighborhood gathering places to find access to information and start matching resources and skills to what is needed” said Cindi Barker of West Seattle, one of Seattle’s Hub Captains. “Power Out, No Bars is the latest in a series of emergency exercises that have helped our membership continually hone their skills and upgrade, deploy, and test their equipment,” said Mark Sheppard, founder and director of ACS. “This is critical to improving our ability to be more effective and be better prepared to face a real emergency or natural disaster. Here are the West Seattle hubs participating: *Pigeon Point Hub, 20th Ave SW & SW Genesee St *High Point Hub at Neighborhood House, 6400 Sylvan Way SW *Fauntleroy United Church of Christ Hub, 9140 California Ave SW
Return to Top	

HEADLINE	**04/26 DHS ends protected status for Nepal**
SOURCE	**https://apnews.com/789fb21af4554eebb78613df17c9e1f5/US-to-end-special-protections-for-9,000-Nepalese-immigrants**
GIST	WASHINGTON (AP) — The Trump administration will end special protections for an estimated 9,000 Nepalese immigrants living in the United States, giving them until June 24, 2019, to leave or find another way to stay in the country, the Department of Homeland Security said Thursday. They were granted that status during the Obama administration after an April 2015 earthquake killed more than 8,000 people in Nepal, and it was extended for 18 months in October 2016. But DHS said that after a review of conditions in the country, Secretary Kirstjen Nielsen concluded the protections were no longer warranted. The “disruption of living conditions in Nepal from the April 2015 earthquake and subsequent aftershocks that served as the basis for its TPS designation have decreased to a degree that they should no longer be regarded as substantial,” DHS said.

	The U.S. created Temporary Protected Status in 1990 to provide a safe haven for citizens of countries affected by war and natural disasters such as earthquakes, floods and hurricanes. The status currently shields several hundred thousand people from 10 countries. It generally includes authorization to work. The decision on Nepal probably will be felt most acutely in New York and the Dallas-Fort Worth area, which had the largest Nepalese immigrant communities in the United States in 2015 with 9,000 each, according to the Pew Research Center. Washington, San Francisco, Baltimore, Pittsburgh and Columbus, Ohio, also have large communities. The decision on Nepal was met with anger from immigration activist, including Amanda Baran of the Immigrant Legal Resource Center.
Return to Top	

HEADLINE	**04/27 Feds: lost track of immigrant children**
SOURCE	**https://apnews.com/a92409ad458742ad952fede5596c36a3/Federal-agency-says-it-lost-track-of-1,475-migrant-children**
GIST	Federal officials lost track of nearly 1,500 migrant children last year after a government agency placed the minors in the homes of adult sponsors in communities across the country, according to testimony before a Senate subcommittee Thursday. The Health and Human Services Department has a limited budget to track the welfare of vulnerable unaccompanied minors, and realized that 1,475 children could not be found after making follow-up calls to check on their safety, an agency official said. Federal officials came under fire two years ago after rolling back child protection policies meant for minors fleeing violence in Central America. In a follow-up hearing on Thursday, senators said that the agencies had failed to take full responsibility for their care and had delayed crucial reforms needed to keep them from falling into the hands of human traffickers. “You are the worst foster parents in the world. You don’t even know where they are,” said Democratic Sen. Heidi Heitkamp of North Dakota. “We are failing. I don’t think there is any doubt about it. And when we fail kids that makes me angry.” Since the dramatic surge of border crossings in 2013, the federal government has placed more than 180,000 unaccompanied minors with parents or other adult sponsors who are expected to care for the children and help them attend school while they seek legal status in immigration court. An AP investigation found in 2016 that more than two dozen unaccompanied children had been sent to homes where they were sexually assaulted, starved or forced to work for little or no pay. At the time, many adult sponsors didn’t undergo thorough background checks, government officials rarely visited homes and in some cases had no idea that sponsors had taken in several unrelated children, a possible sign of human trafficking. Since then, the Health and Human Services Department has boosted outreach to at-risk children deemed to need extra protection, and last year offered post-placement services to about one-third of unaccompanied minors, according to the Senate Permanent Subcommittee on Investigations. But advocates say it is hard to know how many minors may be in dangerous conditions, in part because some disappear before social workers can follow up with them and never show up in court. From October to December 2017, HHS called 7,635 children the agency had placed with sponsors, and found 6,075 of the children were still living with their sponsors, 28 had run away, five had been deported and 52 were living with someone else. The rest were missing, said Steven Wagner, acting assistant secretary at HHS.

	Republican Sen. Rob Portman gave HHS and the Department of Homeland Security until Monday to deliver a time frame for improving monitoring. "These kids, regardless of their immigration status, deserve to be treated properly, not abused or trafficked," said Portman, who chairs the subcommittee. "This is all about accountability." Portman began investigating after a case in his home state of Ohio, where eight Guatemalan teens were placed with human traffickers and forced to work on egg farms under threats of death. Six people have been convicted and sentenced to federal prison for their participation in the trafficking scheme that began in 2013.
Return to Top	

HEADLINE	**04/27 Authorities: Wisconsin refinery fire out**
SOURCE	**https://apnews.com/e1b82b2411c0400da4d3091ffd71ac63/Authorities:-Wisconsin-refinery-fire-out,-evacuation-remains**
GIST	Authorities have not allowed residents back in their homes after crews extinguished a smoky blaze at a northwestern Wisconsin refinery where an explosion injured at least 11 people and forced most of the city of Superior to evacuate. Douglas County officials said Thursday evening the fire at the Husky Energy oil refinery was out and that residents could return home but wait at least two hours before doing so. But late Thursday, Superior police gave another update, saying the evacuation order would remain and be re-evaluated throughout the night. Authorities said a tank of crude oil or asphalt exploded about 10 a.m. Thursday at the refinery in Superior, a city of about 27,000 that shares a Lake Superior shipping port with nearby Duluth, Minnesota. That prompted them to order the evacuation of a 3-mile (5-kilometer) radius around the refinery, as well as a 10-mile (16-kilometer) corridor south of it where the smoke was heading. It was unclear how many people evacuated, but Mayor Jim Paine said most of the city was being evacuated. The refinery is in an industrial area, but there's a residential neighborhood within a mile to the northeast. The corridor downwind to the south of the refinery is sparsely populated. Schools in Superior and nearby Maple, Wisconsin, canceled classes Friday as a precaution.
Return to Top	

HEADLINE	**04/27 Arizona, Colorado teachers 2nd day rally**
SOURCE	**https://apnews.com/fc6c9b239ba341c8905bce5ed71b16b1/Arizona,-Colorado-teachers-rally,-schools-close-for-2nd-day**
GIST	PHOENIX (AP) — Arizona and Colorado teachers plan to don red shirts and descend upon their respective Capitols for a second day in a growing educator uprising. Educators in both states want more classroom resources and have received offers either for increased school funding or pay, but they say the money isn't guaranteed and the efforts don't go far enough. The walkouts are the latest in demonstrations that spread from West Virginia, Oklahoma and Kentucky. On the first day of the historic statewide walkout, around 50,000 educators and their supporters marched Thursday through downtown Phoenix in nearly 100-degree (38-Celsius) heat and swarmed the Capitol grounds. In much cooler Colorado, several thousand educators rallied around the Capitol, with many using personal time to attend two days of protests expected to draw as many as 10,000 demonstrators.

	Lawmakers in Colorado have agreed to give schools their largest budget increase since the Great Recession. But teachers say Colorado has a long way to go to recover lost ground because of strict tax and spending limits. Arizona's Republican governor, Doug Ducey, has proposed 20 percent raises by 2020 and said he has no plans to meet with striking teachers or address other demands. More than 840,000 students were out of school as a result of Thursday's walkouts, according to figures from The Arizona Republic. Most of Arizona's public schools will be closed the rest of the week, and about half of all Colorado students will see their schools shuttered over the two days as teachers take up the Arizona movement's #RedforEd mantle. In Oklahoma and West Virginia, teacher strikes stretched beyond the one-week mark. Organizers say they haven't decided how long their walkout will last.
Return to Top	

HEADLINE	**04/26 Across Europe, Jewish safety fears grow**
SOURCE	**https://www.usnews.com/news/best-countries/articles/2018-04-26/safety-concerns-grow-for-jews-across-europe**
GIST	Late in March, Mireille Knoll, an 85-year-old Jewish grandmother and Holocaust survivor, was found dead – stabbed to death with her body partially burned – in her Paris apartment. Two men in their 20s were placed under formal investigation on charges of murder motivated by anti-Semitism. French interior minister Gérard Collomb told Parliament that one of the alleged killers told the other, "She's a Jew. She must have money." French authorities are still investigating the circumstances of the case, but Jewish advocacy groups across the world have situated the murder in the broader context of rising anti-Semitism in France, and across Europe. For Dr. Moshe Kantor, president of the European Jewish Congress, the slaying is "a sad symbol of what we are returning to." In January, in a speech at the European Parliament, Kantor warned that Europe is no longer safe against anti-Semitism because the last generation of Holocaust survivors and witnesses is dwindling. Knoll's death, he said, is another sign. "There have been far too many of these murders and attempted murders of Jews in France to call them sporadic," Kantor wrote in an email. "This murder should not just appall us, it should serve as a final wake-up call that more must be done not just to protect Jewish communities and institutions, but also all individuals at risk." Lethal violence against Jewish people is certainly not an everyday occurrence, but the brutal murder of a woman who had already experienced the horrors of mass genocide has been particularly painful to the international Jewish community. It follows other shocking anti-Semitic incidents in France, such as the 2012 killing of three Jewish children and a teacher at a Jewish school in Toulouse by an Islamic fundamentalist, and the 2015 murder of four people at a Jewish supermarket, linked to the Charlie Hebdo killings. More recently, a Syrian man turned himself in to German police last week after admitting to using a belt to beat an Israeli man wearing a yarmulke in Berlin. The incident sparked protests this week and – in a nation sensitive to its relations with its Jewish community – has drawn the condemnation of Chancellor Angela Merkel. Knoll's death resonates deeply across France because the country is home to the largest population of Jews in Europe and to the fourth largest such population in the world by country, according to 2015 data from

the independent Pew Research Center. It also is part of a broader trend of growing anti-Semitism and Islamophobia that a European Union report noted more than two years ago.

There is rising concern about the safety of Jewish people and communities in Europe, as the number of violent attacks aimed at Jews in many countries has risen in recent years. Jewish leaders are speculating on the reasons why this may be occurring now. Some, such as Kantor, argue that 73 years after the end of World War II, Europe is no longer inoculated against anti-Semitism. Others blame the rise of populist, nationalist political parties, while still others point to radicalized Muslims, who, according to recent data from the University of Oslo, are most often the perpetrators.

Knoll's murder follows another attack in April 2017, when Sarah Halimi, a 65-year old Orthodox Jewish physician and kindergarten teacher in Paris, was beaten in her apartment and then thrown out a window. Both women had lived alone and had previously complained of anti-Semitic threats, according to Noémie Halioua, a French journalist with the Jewish weekly newspaper Actualité Juive and the author of a new book on the Halimi case.

While racially motivated hate crimes have decreased in France overall, there has been an uptick in anti-Semitic violence in the past year, from 77 incidents in 2016 to 97 in 2017, according to a report released by the Kantor Center for the Study of Contemporary European Jewry at Tel Aviv University in early April. The authors of the study cautioned that the information could not be verified by their criteria.

Is Anti-Semitism Waning in Europe?
The report also found that physical violence against Jewish people around the world dropped by 9 percent from 2016 to 2017, but anti-Semitic sentiment, hate-speech, threats and cyberattacks have become mainstream throughout Europe, they asserted, leading to a "corrosion of Jewish life."

Kantor says anti-Semitic violence has become "an almost daily occurrence in parts of Europe and apparently, Jews no longer feel that they can rely on the preventive actions of the law enforcement authorities to protect them even in their own homes."

The report concludes that the rise of anti-Semitism can be attributed to "the constant rise of the extreme right, a heated anti-Zionist discourse in the left, accompanied by harsh anti-Semitic expressions, and radical Islamism."

The Anti-Defamation League, an American Jewish nongovernmental organization, counts Knoll's death as the 11th anti-Semitic murder in France in the past 12 years. The group estimates that assaults on Jews that take place twice a week on average in France, creating a sense of insecurity for the entire Jewish community.

Sharon Nazarian, its senior vice president of International Affairs, has spent the past several months traveling to European capitals such as Paris, Berlin, Stockholm, Brussels, Budapest and Rome, speaking with Jewish community leaders and government officials.

"What I'm hearing from them is a real nervousness, a feeling insecurity, a lack of safety, both physically and also for their Jewish way of life," said Nazarian in a telephone interview. "It's really unprecedented going back to World War II. A lot of warning bells are going off and red flags are going up and we're very, very concerned."

She says "a loss of a sense of shame that did exist for decades after the war" about anti-Semitic attitudes has contributed to the shift, along with the rise of nativist right-wing politicians, anti-Zionist left wing activists, and scapegoating of Jews for other global problems.

Violent incidents, the Kantor Center report finds, have decreased because of better security and intelligence in protecting Jewish communities. But the report stresses that "it is overshadowed by the many verbal and visual expressions, some on the verge of violence, such as direct threats, harassments, insults, calls to attack Jews and even kill them en masse."

	Alvin Rosenfeld, director of the Institute for the Study of Contemporary Antisemitism at Indiana University and an author of many books on the Holocaust and the perspectives of it, argues that anti-Semitism has never truly left Europe. "The view that knowledge of the Holocaust would somehow be prophylactic, and it would guard against the return of anti-Semitism, seems now to be naive, and I admit that I myself subscribed to that view," he says. "It just isn't the case that Holocaust memory guards against the repeat of Jew hatred." He agrees that the rise of anti-Semitic sentiment stems from a multiplicity of forces. "We're living at a time in which neo-nationalism, neo-nativism, populism, autocracy and theocratic extremisms are all coming to the fore, in some cases with a great rush," he said. "Anti-Semitism, together with hatred against other types of people, flourishes in such a climate."
Return to Top	

HEADLINE	**04/26 Officials: MS-13 'gaming' immigration**
SOURCE	**https://www.washingtontimes.com/news/2018/apr/26/ms-13-gang-members-claim-theyre-underage-gain-acce/**
GIST	MS-13 is paying smugglers to coach gang members on how to game the U.S. immigration system, teaching underage members to claim UAC status — and telling those over 18 to lie and claim they are underage — to try to gain quick, easy access to the U.S., government officials said Thursday. Rep. Peter T. King, a New York Republican, said his district is such a hotbed of MS-13 activity that authorities are "right now digging for bodies within a mile of my house." He said some families are forced to facilitate gang members' arrivals and are pressured by gangs to become sponsors and claim the children when they arrive. Homeland Security Secretary Kirstjen Nielsen confirmed the pipeline. "They recruit young children, they train them how to be smuggled across our border, how to then join up with gang members in the United States," she told Congress. The government this week detailed such a case from this month in Arizona, where Border Patrol agents nabbed an 18-year-old from El Salvador. He first claimed to be underage to try to claim UAC status. Under questioning, he acknowledged he was an adult and was part of MS-13 — though he insisted he was trying to leave the gang. Unaccompanied alien children — those who arrive at the U.S. border without their parents — are among the trickiest populations of illegal immigrants. They began to surge toward the U.S. in 2012 and crested in 2014, overwhelming an Obama administration that was ill-equipped to handle them. In addition to gangs, some UAC were turned over to criminals, who forced them into labor or otherwise abused them. More than five years into the crisis, the UAC numbers are once again rising — and the administration is still struggling to get a grip on matters, as officials made clear in hearings Thursday on both sides of the Capitol. While Ms. Nielsen begged House lawmakers to close the loopholes that she said invite UAC and others to test U.S. immigration policy, Homeland Security and Health and Human Services officials were being grilled by senators about why the government is unable to keep track of the children once they are in the U.S. Steven Wagner, an acting assistant secretary at HHS, said of 7,635 UAC that the department tried to check

	in with last year after their first 30 days with their sponsors, they found 28 had run away and 52 had ditched their sponsors to move in with others. More striking, though, were the 1,475 UAC whom the department "was unable to determine with certainty the whereabouts of" just 30 days after they had been placed in those homes. "You are the worst foster parents in the world. You don't even know where they are," said Sen. Heidi Heitkamp, North Dakota Democrat. Losing track of UAC matters, both for the children's well-being and for the ability of the government to push them through the immigration system, getting them a hearing and deciding if they should be deported or granted permanent status. Nearly 60 percent of all UAC don't show up for their hearings. Children who don't show up for their hearings are essentially free and clear. Neither HHS nor Homeland Security said they pursue UAC who skip out on their hearings. Indeed, the latest numbers show that just 3.5 percent of UAC who came to the U.S. during the surge are deported, Ms. Nielsen said. Government officials pointed fingers at each other, and lawmakers said they were getting fed up after Homeland Security and Health and Human Services couldn't tell the Senate's chief investigative panel when they will complete a months-overdue joint cooperation plan. Part of the problem is that the legal framework for UAC is disjointed at best. Children from Mexico can be deported quickly, but those from noncontiguous countries must be processed by Homeland Security and then turned over to HHS, which holds them in government-run dorms until sponsors can be found. Sen. Rob Portman, an Ohio Republican and chairman of the Senate investigative panel, said HHS has a signed agreement with each UAC sponsor, who agrees to make sure the children show up for their hearings. But he said HHS doesn't even know when they skip the hearings. "We have no mechanism for enforcing the agreement if they fail to show up," Mr. Wagner confirmed. "Obviously a red flag when a child fails to show up for a hearing. I think we've identified this morning so many parts of the system that simply aren't working for the children or for our immigration system," Mr. Portman said. The amount of information the government didn't know at the Senate hearing was stunning. Mr. Wagner couldn't say how often his department alerts local police about potential dangers they should be aware of in some homes, nor could he say how often fraudulent documents are used. He couldn't detail the criteria that foster parents are required to meet to accept children and couldn't even say how many of the sponsors the UAC are being delivered to aren't U.S. citizens.
Return to Top	

HEADLINE	**04/26 Norovirus closes Tacoma restaurant**
SOURCE	**http://www.thenewstribune.com/entertainment/restaurants/tnt-diner/article209939349.html**
GIST	Another suspected norovirus outbreak has sickened diners in Tacoma. The outbreak is connected to

	Foley's on the Green, the restaurant and sports bar at the Meadow Park Golf Course in Tacoma at 7108 Lakewood Drive W. Eight reports have been made for suspected norovirus. The Tacoma-Pierce County Health Department closed Foley's on Thursday for at least 24 hours or until the restaurant is thoroughly cleaned and sanitized. Jason Follen, owner of the restaurant, said he and his employees were at work Thursday doing just that. They're also searching for a potential cause for the outbreak. He said he's called some of the food-service companies that supply his restaurant to see if outside contamination is possibly to blame. "I have good employees, and I'm confident that this is just an isolated bad luck incident and we're just shocked," said Follen. The health department also is investigating what might have caused the outbreak. "We're in the middle of the investigation now," said Health Department spokeswoman Edie Jeffers. She said reports came in April 23, 24, and 26.
Return to Top	

HEADLINE	**04/27 Koreas leaders in diplomatic dance**
SOURCE	**https://www.nytimes.com/2018/04/27/world/asia/north-korea-south-border.html?hp&action=click&pgtype=Homepage&clickSource=story-heading&module=b-lede-package-region&region=top-news&WT.nav=top-news**
GIST	HONG KONG — A carefully choreographed diplomatic dance at the Korean border added a surprise extra step on Friday, instantly turning a moment destined for the history books into a viral meme for the social-media era. The surprise moment in which Kim Jong-un, the North Korean leader, encouraged President Moon Jae-in of South Korea to step over the border to the North's side became one of several images that displayed both countries' understanding of the propaganda value of political theater. After a year in which tensions between the two countries reached an acrimonious pitch not seen in decades, the two leaders were careful to publicly signal a new era of rapprochement. Smiling broadly at each other, the men took their time shaking hands as Mr. Kim stepped gingerly over the concrete slab that marks the border between the two countries, becoming the first North Korean leader to set foot in the South. Knowing that photos and video of their meeting would be broadcast around the world, even their clothing — veritable costumes — was chosen to project a message. For Mr. Moon, a dark business suit was paired with a light blue tie that echoed the hue used in the Korean Unification Flag, which the countries use when competing together as single team at international sporting events. Mr. Kim wore an austere black Mao-style suit, a message to his citizens that despite being in enemy territory he was still committed to the ideals — and dress — of his grandfather Kim Il-sung, North Korea's founder, who ordered the 1950 invasion of the South that started the Korean War. Once on the South side of the Demilitarized Zone, the stretch of land that makes up the border and in which the summit meeting took place, Mr. Kim inspected a military honor guard. Though the DMZ is heavily fortified and security was tightened for the visit, the honor guard's soldiers carried spears and

	swords, instead of rifles. They were dressed in 19th-century costumes, worn at a time when Korea was a unified empire. Even the décor inside Peace House, the building in which the meeting took place, was chosen for its political optics. In the run-up to the talks, workers hung paintings of Mount Kumgang, which straddles the border and is an important symbol to Koreans in both countries. The table and chairs inside the meeting room were also carefully designed with a pattern evoking two bridges coming together. At the table was Mr. Kim's sister, Kim Yo-jong, the only woman in the delegation. Ms. Kim's stature has risen since she represented the North's government at this year's Winter Olympics in Pyeongchang, South Korea. That visit was widely seen as an opening gambit toward a détente, and Ms. Kim was widely credited with softening her country's image. At Peace House, Mr. Kim signed a guest book, leaving a message guaranteed to be photographed, tweeted and deconstructed by political analysts. "A new history starts now," he wrote. "An age of peace, from the starting point of history."
Return to Top	

HEADLINE	**04/26 'Breathtaking potential implications' lawsuit**
SOURCE	**http://mynorthwest.com/967315/washington-native-american-tribes-salmon-case/**
GIST	Former Washington state Attorney General Rob McKenna says it's the most important case Washingtonians have never heard about, yet its results could dramatically change how government works in the Pacific Northwest. "It really is breathtaking in its potential implications," McKenna told KIRO Radio's Dave Ross. The issue surrounds the influence Native American tribes have on local and state governments. While the case itself centers on culverts that affect salmon runs, McKenna argues there is legal engineering going on that could place the tribes in a position to co-govern much of the state. "It's not because most tribal members depend on fish to make their living; some do, but most don't," he said. "It's because it's a way to restore sovereign control over lands they used to own. I appreciate that objective. I understand why they are pursuing it. But it's not what the treaties were about. And it's not something that the State of Washington or its local governments can accept." The right to salmon The legal relationship between Washington state, the United States government, and the Northwest's Native American tribes dates back to the mid-1800s when a series of treaties were signed. Those treaties essentially detailed who had a right to what — which lands were exchanged and where tribes could fish. In short, tribes were granted the right to always fish where they traditionally had. That notion was upheld in the 1970s Boldt decision. But a lingering treaty issue has led to the United States Supreme Court. "The treaties grant the tribes a right, in perpetuity, to access their traditional fishing grounds," McKenna said. "The two questions that have been litigated over the last 40-plus years have to do with how much of the fish they are entitled to. In the Boldt decision, it was decided they are entitled to half. Then, in this case, that went to the Supreme Court, the question is what happens when there are fewer fish to catch because of something the state has done. In this case, building culverts under state highways, and on park land, and lands owned by the State of Washington."

	Such culverts can choke off streams that salmon use to spawn, threatening the number of fish that the tribes historically relied upon. When McKenna was attorney general, he repeatedly offered to settle the culvert case issue. Many culverts under natural resources and state parks have already been replaced. And the Washington State Department of Transportation has been systematically replacing them. McKenna said he offered a fixed schedule to replace all remaining culverts. But those offers were consistently turned down. McKenna says this is because there is a larger plan in the works. Native American tribes and treaties McKenna says that Washington state tribes want to establish that their treaty rights to fish give them a role and a right to any decision that affects the fish population. Such authority could touch many governing decisions from water rights and permits, to land use policy, etc. “It was very telling when the tribes filed their brief through the United States government in the Supreme Court that they shifted from the traditional standard in this case – what would be the right amount of fish to ensure the tribes a ‘moderate living’ – which are the words that have been used for decades,” McKenna said. “They’ve shifted to this idea of a ‘substantial degradation of the fish supply,’ which is a new standard that we haven’t seen before.” “And it really goes to what I’m saying; they want to go to a guaranteed supply of fish, and therefore, a say in anything that affects the number of fish,” he said. “There is a lot of agreement that culverts should be replaced. There is not an agreement that tribes are co-sovereign with state and local government over any decision that can affect the number of fish.” McKenna argues that, on one hand, it’s true that the tribes were not signing up for treaties under which the state could block every salmon-bearing stream with a road or a highway. But at the same time, the government of the day was not agreeing to give tribes a co-sovereign role in the management of lands and waters. “No one thought there would ever be a question about the amount of fish (back then),” McKenna said. “There was so many salmon and natural resources, people thought they were inexhaustible. Of course, they were proved to be wrong.” Other leaders in the region have argued that the Supreme Court should side with the tribes, such as King County Executive Dow Constantine.
Return to Top	

HEADLINE	**04/26 UN: 10 aid workers missing South Sudan**
SOURCE	**http://abcnews.go.com/International/wireStory/10-aid-workers-missing-war-torn-south-sudan-54743716?**
GIST	Ten aid workers have gone missing in civil war-torn South Sudan just days after another group of humanitarians was abducted by gunmen, the United Nations said Thursday. The statement said three U.N. staffers and seven aid workers, all of them South Sudanese, went missing early Wednesday when their convoy driving from Yei town to Tore in Central Equatoria disappeared. The aid workers are with South Sudanese Development Organization, ACROSS, Plan International and Action Africa Help. The U.N. humanitarian coordinator for South Sudan, Alain Noudehou, condemned the latest attack against colleagues. This is the third time aid workers have been held by armed groups in the last six months alone,

	the statement said. Seven local aid workers seized by opposition forces earlier this month in the same area were later freed. Two other local aid workers were killed in a separate incident this month in Unity state. "We are deeply concerned about the whereabouts of these humanitarian workers and are urgently seeking information about their well-being," Noudehou said. South Sudan is one of the world's most dangerous places for humanitarians. At least 98 have been killed since the civil war began in December 2013, most of them local workers.
Return to Top	

HEADLINE	**04/26 Israel denies killing scientist in Malaysia**
SOURCE	**http://abcnews.go.com/International/wireStory/latest-israel-denies-killing-palestinian-malaysia-54746892?**
GIST	Israel's defense minister is denying that his country killed a Hamas-affiliated scientist who was gunned down last week in Malaysia. Avigdor Lieberman told the Arabic news site Elaph that "we did not assassinate him." When asked in the interview on Thursday who killed Palestinian engineer Fadi al-Batsh, the minister said: "Ask James Bond ... maybe James Bond killed him like in the movies." Al-Batsh, an electrical engineering lecturer at a Malaysian university, was gunned down by two men on a motorcycle as he was on his way to a mosque on Saturday. In Gaza, Hamas leaders and relatives are waiting at the Egyptian border for his body. Hamas, the militant Islamic group that rules Gaza, accuses Israel of assassinating al-Batsh. He is to be buried Friday at a ceremony led by Ismail Haniyeh, Hamas' top leader.
Return to Top	

HEADLINE	**04/26 Israel warns will strike back if attacked**
SOURCE	**http://abcnews.go.com/International/wireStory/israel-strike-tehran-attacks-tel-aviv-minister-54745743?**
GIST	Israel's defense minister said in an interview carried by an Arabic news site Thursday that his country will strike back if attacked by archenemy Iran. "We hear many (Iranian) threats ... but if they attack Tel Aviv, we will strike Tehran," Avigdor Lieberman told Elaph. The interview was published Thursday while Lieberman was in the United States for talks with defense officials. There has been a spike in hostile rhetoric between the bitter rivals since an airstrike on a military base in Syria that Iran and Russia blamed on Israel earlier this month. Seven Iranians were killed in the strike on Syria's T4 air base. Israel has neither confirmed nor denied carrying out the strike. Iran has threatened to respond.
Return to Top	

HEADLINE	**04/26 Toronto hospital 'calm, in organized chaos'**
SOURCE	**http://www.cbc.ca/news/health/sunnybrook-hospital-trauma-nurses-doctors-1.4635124**
GIST	Miranda Lamb's day was already busy; the trauma nurse at Toronto's Sunnybrook Health Sciences Centre was dealing with a unit that was overcapacity, all of its beds full. But when a colleague with emergency medical services approached her with news that "something big had happened on the street," Lamb knew what had to be done. The hospital, which is Canada's largest trauma centre, was in "Code Orange" — an emergency code that notifies staff of a mass casualty event. "We try to keep it very calm," Lamb said. "It's a calm, organized chaos. Everybody just goes into their role; everybody steps up." By mid-afternoon Monday, Sunnybrook had received 10 victims from Toronto's deadly van attack, which had played out in minutes along a two-kilometre stretch of nearby Yonge Street, less than 10 kilometres away from the hospital's main campus. Two people were pronounced dead on arrival, five remain in critical condition, and three are listed in serious condition. The tragedy marked the country's second big catastrophe this month, leaving 10 dead and another 14 injured. Two weeks earlier, a bus taking the Humboldt Broncos junior hockey team to a playoff game in Saskatchewan collided with a transport truck, killing 16. As Canadians increasingly worry about an overburdened health-care system, with crowded hospitals and overstretched staff, hospitals of all sizes are showing they still have a remarkable ability to respond to unexpected disasters with impressive efficiency. "What we do is transform chaos into calm," said Dr. Alan Drummond, with the Canadian Association of Emergency Physicians. He said that the way first responders, nurses and doctors were able to leap into action in both a large urban centre, like Toronto, and a rural setting, like in Saskatchewan, speaks highly of the level of professionalism in the pan-Canadian emergency experience. "This is what they're trained to do, this is what they live to do," said Drummond, who is also an ER doctor at the Perth and Smiths Falls District Hospital in eastern Ontario. Training for such mass casualty events is always ongoing at Sunnybrook, says the hospital's surgeon-in-chief Dr. Avery Nathens. "Every drill that we have has made us a little bit better at responding. There's always opportunity for improvement, [but] what we've learned from the past year through the drills was helpful for what came across to Sunnybrook." The hospital has been running mock Code Oranges for "several months" to prepare for events such as this, Lamb said. "How to manage them, how to go in action. But in addition to that, the trauma teams here are trained in taking care of critically ill patients in the initial stages of trauma — in what we call the critical hour," she said. Sunnybrook nursing staff learn how to deal with trauma patients through a mandatory trauma nursing course. And all staff go through something called a "tabletop exercise," meant to bring together teams from across the hospital to run through a mass casualty scenario.

	Unlike a mock Code Orange, this exercise doesn't involve simulated patients; rather it's discussion-based, with teams talking through in detail how they'd respond. After tragedies of Monday's magnitude, staff are debriefed — an exercise that encourages everyone to openly assess their teams and the hospital's performance to see what, if any, lessons can be learned. Trauma nurse Cristina Choy called the experience, including the number of victims and the extent of their injuries, "unimaginable." "I think it is very important to debrief after any situation, especially what happened [Monday]," she said. "I think debriefing helps us [with] what went well, what didn't — but also to get things off our chest as nurses. "A lot of the times we just bottle things up and that's not good." Nathens said he knows that staff will be affected by a tragedy like this. "And there will be a lot of debriefing to understand how we can better support our own staff and how we can do this next time, should it ever happen again." After a pause, he adds: "And it likely will." As for Drummond, he said he has nothing but praise for Canada's health-care workers, especially those who responded to the tragedies in Saskatchewan and Toronto. "Both of these experiences have shown that Canadians should have confidence in their emergency-care system and should be proud of the people that work there."
Return to Top	

HEADLINE	**04/25 Active shooter scare at Fort Bragg**
SOURCE	**http://myfox8.com/2018/04/25/poorly-coordinated-exercise-prompts-active-shooter-scare-at-fort-bragg/**
GIST	FORT BRAGG, N.C. — A “poorly-coordinated exercise” resulted in an active shooter scare at Fort Bragg Wednesday afternoon, according to Fort Bragg Public Affairs Officer Tom McCollum. The Soldier Support Center was evacuated after Fort Bragg emergency services got several calls about an active shooter. Personnel were advised to evacuate or barricade themselves in their offices. First responders learned the active shooter situation was a drill that had not been coordinated with Fort Bragg officials. The drill took place on the third floor of the Soldier Support Center, where several agencies are located, according to the Fayetteville Observer. It is unclear what agency was conducting the drill.
Return to Top	

HEADLINE	**04/24 Lessons learned Vegas shooting**
SOURCE	**https://www.phe.gov/ASPRBlog/Lists/Posts/Post.aspx?List=f59454e5-a08d-4a13-9abe-0d31ef99f1af&ID=308&Web=e1195e40-c916-4c28-aa5a-de2eda4302e4**

GIST

On October 1, 2017, during the Route 91 Harvest Music Festival on the Las Vegas Strip, a gunman opened fired from the 32nd floor of a nearby hotel on the crowd of concertgoers. He fired more than 1,100 rounds leaving 59 dead and 527 injured.

Recently, ASPR staff spoke with responding agencies from the Las Vegas shooting to help identify lessons learned that can help other communities, specifically members of the nation's 476 health care coalitions, prepare for, respond to, and recover from these traumatic, no-notice incidents. Here are some of those lessons:

Lesson One: Prepare for Non-triaged Patients. EMS transported fewer than 20% of the victims from the Las Vegas shooting; most were self-transported or transported to healthcare facilities. Healthcare facilities must be ready to provide triage services at or outside the hospital to quickly identify where patients should be treated, and they should collaborate with EMS and other healthcare facilities throughout the region, as part of a health care coalition, to transfer patients based on acuity and available resources. This is especially important for trauma centers that may receive many "walking wounded" patients and hospitals that do not provide trauma services that may initially receive critically injured patients. EMS and other community partners should consider developing a re-distribution plan to move casualties between hospitals.

Lesson Two: Identify and Conduct Drills Using Personnel Notification Tools. Immediately after hearing about the shooting, many healthcare providers arrived at their respective hospitals to help. Make sure your facility has a plan and a tool or messaging solution in place to rapidly notify staff who should come to the hospital and when, based on the needs of the injured and the need for providing round-the-clock care, potentially for days to come. Be aware that no-notice incidents often overwhelm landline and cellular networks.

Lesson Three: Anticipate Challenges in Intake and Throughput. Immediately following the shooting, one hospital received more than 215 patients. Treating that number of patients with limited staff and resources presents inherent challenges. A disaster plan should address which areas of your facility are appropriate for use as expanded emergency department space; how best to group arriving patients, such as by the type and severity of injuries; moving non-incident patients to other areas of the hospital; modifying surgery schedules; and discharging or transferring non-emergent patients.

Lesson Four: Expand Traditional Healthcare Roles to Address Patient Surge. Healthcare facilities should consider having specialty providers and other personnel assume non-traditional roles to help address patient surge. For example, consider using anesthesiologists to manage secondary triage and using pediatric providers to care for ambulatory victims. Take advantage of EMS providers who may be at your facility and willing to assist. Also, consider dedicating certain personnel—respiratory therapist, pharmacist, hospitalists, and intensivist—to only manage the patients coming in from the incident.

Lesson Five: Coordinate Communications with Area Hospitals. Be Ready to Shelter Patients in Place. Community triage systems may be challenged in the immediate aftermath of a no-notice incident. All healthcare facilities in the area should prepare to treat what you can, coordinate patient transfers with other healthcare facilities, and shelter patients in place. Trauma centers may need to prioritize transfers due to the lack of EMS or trauma center resources. Traffic restrictions and misinformation resulting from the event may delay or prevent the timely transfer of patients.

Lesson Six: Review Your Existing Mass Fatality Plan. Determine if your existing mass fatality plan is adequate for a mortuary surge. Consider other areas of your facility where you can expand your mortuary space. Since the coroner or medical examiner may need to visit multiple hospitals after a mass casualty event, prepare for delays in the identification and notification processes. Remember: A no-notice incident resulting from an active shooting situation is also a crime. Collect evidentiary materials from patients and their clothing as per local standards.

Lesson Seven. Incorporate Family Notification in Planning Efforts. Expect loved ones to show up looking for patients, even if those patients are not being cared for by your facility. Designate a location

	away from treatment spaces where loved ones can wait and establish a process to provide regular updates even if there is no new information to give. Provide patient status information on a case-by-case basis in a room separate from the waiting location. Ensure social workers, clergy, and case managers are available to provide mental health support. ***Lesson Eight. Plan for Intense Media Interest.*** The media will want access to your hospital, your staff, and patients and their families. Pre-identify a media staging area, away from where patients are entering/exiting the hospital. Have public affairs staff available to help coordinate media interviews utilizing hospital spokespersons. Provide regular updates even if there is nothing new to report. Know the story you want to tell, coordinate with other hospitals and responding organizations, and be consistent in messaging. "Mass casualty emergencies require a coordinated response involving the entire healthcare community," said Melissa Harvey, director of ASPR's Division of National Healthcare Preparedness Programs. Ms. Harvey oversees ASPR's Hospital Preparedness Program (HPP), the only source of federal funding for health care system readiness.
Return to Top	

HEADLINE	**04/26 Homebuyers looking outside Seattle**
SOURCE	**http://komonews.com/news/local/buyers-look-north-and-south-of-seattle-as-average-home-price-soars-to-nearly-800000**
GIST	SEATTLE - For Melissa Anderson cruising real estate web sites has become an obsession. Newly married and a native of the Pacific Northwest, the 28-year-old who works in medical sales said she and her husband are ready to grow their family, or at least add another dog, and they need more space. "Owning a house is a dream for me," Anderson said. But on Thursday, Zillow released the latest round of bad news for Seattle's already tough housing market – inventory is down and prices are up. Zillow said more than 41 percent of homes for sale in Seattle are priced higher than $870,000. Inventory of homes for sale is down and the median home values rose 14.8 percent, according to Zillow. "For Seattle you're seeing the higher end of the market and the lower end of the market are appreciating right around 15 percent annually, which that in itself is crazy," said Svenja Gudell, Zillow Chief Economist. Seattle, according to Zillow, is the third fastest appreciating housing market and third fastest appreciating rental market in the country. West Seattle Realtor Natalie English isn't surprised by the statistics. "I would say an average of over 20 percent over list price is kind of what I'm seeing. If a house is listed, say, 925 it's probably going to go for at least a million," said English, who is a broker for Windermere. Standing in the living room of a sunny home in West Seattle's North Admiral neighborhood Thursday, English said she was surprised she hadn't made a sale on it yet. English said the home, listed for just under $1.2 million, has sat on the market six days - she expects it will sell soon. "I would say six says is my average days on the market before we get multiple offers," English said. While Zillow said inventory is down 16.1 percent over the past year, English said she's having her busiest year in her 16 years working in real estate. She said there are plenty of luxury home buyers and they move

	fast. But for people who can't afford a home over a million dollars, English said she has seen lots of growth in home sales in Sammamish, Duvall and further outside the city limits. "They're having to stretch out a little bit," English said. "You're either going north of Seattle or south of Seattle where the prices are somewhat affordable." After seeing house prices skyrocket in her beloved Queen Anne neighborhood, Anderson said she has expanded her search as far out as Kitsap County.
Return to Top	

HEADLINE	**04/26 DOL: 100+ salons w/violations**
SOURCE	**http://www.khq.com/story/38051899/100-salons-in-washington-have-license-sanitation-or-safety-violations**
GIST	KHQ.COM - More than 100 salons in Washington state either failed safety or sanitation inspections, or had license violations in the last year from the Washington State Department of Licensing. If you think these salons are required to post these violations publicly, think again. Unlike restaurants, there's no letter grade at the door that can tell you if the services inside have been deemed safe or violation free. Violators receive a fine from the state and then continue running the business as usual. To find out if your salon, or any other business place has received a violation you can visit the Washington State DOL website. The DOL posts all violations on their website under the "professions" section for numerous professions. Salon violations can be found under the "cosmetologists" section.
Return to Top	*Click on link to view DOL listing of salons with violations:* http://www.dol.wa.gov/business/disciplinary/disciplinarycosme.html

HEADLINE	**04/26 Homeless camp Green Lake to move**
SOURCE	**http://q13fox.com/2018/04/26/unsanctioned-encampment-accused-of-terrorizing-green-lake-residents-is-moving-out-looking-to-settle-elsewhere/**
GIST	SEATTLE -- Several neighbors who say a homeless encampment has taken over their Green Lake neighborhood met for the first time on Thursday. "When I am home alone, I don't feel that safe," Betsy Peto said. Residents say when the tents moved in overnight a stone's throw away, they didn't know what to think. Now they are just mad. Neighbors have vented on social media and with each other, but many stayed silent, fearing retaliation. Now many are fed up and willing to talk about it. "Bowel movement on her driveway last week and then a needle on her driveway the other day," Phil Cochran said of a neighbor's home. Residents along 5th and 58th say they are dealing with theft, needles, defecation and now aggressive behavior from some of the campers. "Verbally abusing, walking past calling my wife human trash and garbage for no reason whatsoever," Mike Liddell said. That is just the beginning, residents say. A couple of times they've seen people at the camp throwing

	things over the wall next to the encampment, they say. Over that wall is I-5 and dozens of what appears to be stolen bicycles now left abandoned in a wooded area next to I-5. "They basically have a bicycle store house going; yes, it's shocking. I had no idea and that they operate so openly," Liddell said. Liddell and his neighbors say they have repeatedly reached out to Seattle city leaders for nearly two months. "We haven't had any useful info from them so far, all we understand is that council has told the police to back off," Liddell said. "I am not trying to criminalize the homeless; I am against people breaking the law," Peto said. Shortly after interviews with neighbors, Q13 News saw city crews posting eviction notices around the encampment site. The Neighborhood Action Coalition, the group that helped move the campers to Green Lake, is against the eviction. But Matt Lang, a member of the group, acknowledged to Q13 News that things have gotten unruly. "It's caused a lot of tension in that neighborhood, not best for anyone for that camp to remain," Lang said. Lang says he will help move the camp somewhere else this Sunday but a location has yet to be determined.
Return to Top	

HEADLINE	**04/27 Experts: US unprepared for biothreats**
SOURCE	**https://www.hstoday.us/subject-matter-areas/pandemic-biohazard/country-a-lot-more-ragile-than-we-realize/**
GIST	The nation is critically underprepared to confront transnational biological threats ranging from DIY bioterror agents to natural pathogens that outpace current pharmaceuticals and overwhelm medical facilities, the Blue Ribbon Study Panel on Biodefense heard at a Wednesday event at the Hudson Institute. James Lawler, a retired Navy commander whose experience includes serving as director for medical preparedness policy on the National Security Council and director for biodefense policy on the White House's Homeland Security Council, warned that the country is "woefully unprepared for these biological threats" in an increasingly interdependent world. "Events halfway around the world have rapid effects," he said, and the nation suffers from a "lack of threat awareness and poor situational awareness as it comes to biological threats." Problems include "excruciatingly slow and moribund" programs that rely too much on "backwards engineering" of the last big threat along with insufficient staffing and not enough human intelligence on biological programs, as well as a "lack of situational awareness in day-to-day health activities." Lawler stressed that there are "still significant problems connecting the clinical world with the public health world," while the ability "to be able to understand those events in real time is critical to being able to defend ourselves in rapidly evolving events." As genetic engineering continues to evolve, he warned, the threat will "exponentially" increase with "significant potential for malevolent use."

	"Innovation is going to be the key to moving us ahead," he said, with a need "to think beyond the linear approach we're using now." "If you're the kind of person who lies awake at night thinking about problems, this is one of the problems you should be thinking about… we're now in the era of the iPhone 10 and we're still using a flip phone." Kenneth Luongo, president and founder of the Partnership for Global Security, echoed that the U.S. "remains woefully underprepared" for a biological attack or a "new intensity level" of pathogens. He cited Rhode Island hospitals being overwhelmed by flu patients this past winter to the point of having to transfer overflow patients, "and this is an infectious disease that we prepare for every year." Better modeling is needed to map the potential spread of disease, he said. Synthetic biology presents new challenges from a risk perspective as new biological systems can be used for malicious purposes, he warned. Because of the natural lack of transparency about biological programs from authoritarian regimes, it "falls to the intelligence community to determine what's happening" in research programs with "serious questions" like Russia — where Luongo has "no doubt" there's an active biological program with weapons potential. Even though the lack of a biological attack has lowered the priority of addressing biological threats, Luongo warned "that's a mistake." Ridge's co-chairman on the Blue Ribbon Study Panel, former Sen. Joe Lieberman (I-Conn.), said later in the conference that while he's worried about a bioterror attack the impact of an infectious disease pandemic could be worse as "the potential for devastation is great." Former USAID Director Andrew Natsios, director of the Scowcroft Institute of International Affairs, told the panel that the country is "a lot more fragile than we realize" when it comes to emergency response, and the ebola crisis demonstrated the need for several central points at which decisions can be made rapidly. "Time is of the essence — the longer the delay, the more people could die," he said. Natsios warned of the consequences of a lack of U.S. leadership in the international system. "We are sort of like Jimmy Stewart — we are going to see what the world looks like without that honorable man in the movie," he said, referencing "It's a Wonderful Life." With deficits in drug development, he suggested expanding upon the Gavi Vaccine Alliance model in which pharmaceutical companies are promised that if they mass produce, the products will be marketed through NGOs and the UN. "Do not reinvent the federal organization wheel," he suggested, while emphasizing the need for coordination. "Do not try, in cases of international aid programs, try to transplant what works well in a Western country to a developing country." And, Natsios recommended, "do not confuse emergency response with other biomanagement issues" – coordinating before the emergency and, once the event takes place, decentralizing to the lowest levels "or we won't get there in time."
Return to Top	

HEADLINE	**04/24 Banner year for Seattle, King Co. tourism**
SOURCE	**https://www.seattletimes.com/business/economy/a-banner-year-for-tourism-in-seattle-and-king-county/**
GIST	Cruise season began last week with the arrival of Norwegian Cruise Line's Norwegian Sun.

	The Port of Seattle projects more than 1.1 million cruise passengers this year, ahead of last year's record. Alaska is the largest destination for cruise ships. Seattle will be the largest cruise port on the West Coast for the second year in a row. Cruise passengers make up an important part of the tourism economy here, spending money in town before and after their voyages. But they're far from the only drivers. Nearly 40 million visitors came to the city and county last year, according to a recent report from Visit Seattle, the 1,000-member nonprofit tourism marketing organization. That's up 2.6 percent from the previous year and marks the eighth straight year setting a record. Overnight visitors grew by 3.9 percent to nearly 21 million. Tourism Economics and Longwoods International estimate that visitors pumped $7.4 billion into the regional economy. Travel and tourism jobs were up 27 percent to more than 76,000 (about 5.6 percent of all employment in King County. Tom Norwalk, president of Visit Seattle, told me the region also "had incredible growth from international business. And this is despite being underserved by international (air) carriers. We've been adding (flights) but there is more we can be doing." International visitors tend to spend more and stay longer than their domestic counterparts. To encourage growth in tourism from overseas, Visit Seattle has marketing reps in Asia, Europe and Australia. The organization benchmarks the tourism sector here against 14 other U.S. cities, getting weekly updates. With long summer days, numerous attractions and the gateway to the Northwest's scenic beauty, Seattle is a natural destination for tourists. Leisure demand was once seasonal, but now we're attracting visitors year-round. Business travel is an important element, too, both corporate and conventions. Norwalk is hoping a deal can be completed for expansion of the Washington State Convention Center. "We're outperforming other destinations for how we utilize the convention center" he said. "But we need the second building… There's incredible demand for Seattle as a meeting destination. Groups sign contracts for years out."
Return to Top	

HEADLINE	**04/27 US, Israel heat up rhetoric on Iran**
SOURCE	**https://www.cnn.com/2018/04/27/politics/us-israel-iran-dangers/index.html**
GIST	Washington (CNN)US and Israeli officials issued tough warnings about Iran's activities in Syria and beyond on Thursday, in the lead-up to President Donald Trump's May 12 decision on whether to stay in the Iran nuclear deal. The steady drumbeat appeared to reinforce signals Trump has been sending about his intent to leave the deal. And in the absence of any clear sign the White House has a "day after" plan, there are deepening concerns in some quarters that White House policy toward Tehran may be shifting from denuclearization to regime change. "I think we are not moving toward a new agreement," said Clement Therme, a Bahrain-based research fellow for Iran at the International Institute for Strategic Studies. "I think we are moving toward a regime change policy in the US." US and Israeli officials laid out a litany of examples of malign Iranian behavior on Thursday. Some laid

	the ground for potential Israeli action against Iran within Syria. Others warned the conflict could spread from there. Speaking to lawmakers, Defense Secretary James Mattis said that Iran is bringing in increased amounts of weaponry to Syria, and suggested that Iran intends to attack Israel. Mattis said Iran's proxy activities in Syria are driving a significant risk of escalated conflict that could engulf the region. Privately, US military officials are warning of the potential for more direct confrontation between Iran and Israel that could spiral out of control. "The potential for escalation has grown," one defense official told CNN's Barbara Starr. The Pentagon is publicly trying to emphasize that any military moves by Iran "would take us where we don't want to go," the official said. "There is serious concern this could escalate." In New York, Nikki Haley, the US ambassador to the UN, told the Security Council that Iran is the patron and protector of groups that use human shields, "part of Iran's overarching efforts to destabilize the region." Danny Danon, Israel's ambassador to the UN, reminded the Security Council that the threats posed by Hezbollah, Hamas and Syria's Assad regime have one common source. "The Iranian regime is the dangerous thread that ties these threats together," he said, before he went on to denounce the Joint Comprehensive Plan of Action, as the nuclear deal is formally known.
Return to Top	

HEADLINE	**04/27 Koreas agree: end war, denuclearize**
SOURCE	**https://www.bloomberg.com/news/articles/2018-04-27/two-koreas-agree-to-end-war-this-year-pursue-denuclearization**
GIST	North Korean leader Kim Jong Un and South Korean President Moon Jae-in agreed Friday to finally end a seven-decade war this year, and pursue the “complete denuclearization” of the Korean Peninsula. The two leaders embraced after signing the deal during a historic meeting on their shared border, the first time a North Korean leader has set foot on the southern side. They announced plans to formally declare a resolution to the war and replace 1953 armistice that ended open hostilities into a peace treaty by year’s end. “We have agreed to share a firm determination to open a new era in which all Korean people enjoy prosperity and happiness on a peaceful land without wars,” Kim said, in his first remarks in front of the global press since taking power in 2011. The two sides “confirmed the common goal of realizing, through complete denuclearization, a nuclear-free Korean Peninsula.” “South and North Korea agreed to actively seek the support and cooperation of the international community for the denuclearization of the Korean Peninsula,” according to the statement. It didn’t elaborate on what that would entail. “The commitment to ‘complete denuclearization’ is ambiguous, and subject to different interpretations,” said Youngshik Bong, a researcher at Yonsei University’s Institute for North Korean Studies in Seoul. “It can be interpreted as North Korea getting rid of all warheads, or North Korean demands on the U.S. military in South Korea.” The agreement follows a rapid thaw of tensions on the peninsula after a flurry of North Korean missile tests and a hydrogen bomb detonation last year. Kim plans to meet U.S. President Donald Trump soon, which would be the first summit between a North Korean leader and a sitting American president.

Return to Top

HEADLINE	**04/26 Army accepts recruits w/behavior issues**
SOURCE	**https://www.usatoday.com/story/news/politics/2018/04/26/army-issues-waivers-1-000-recruits-history-bipolar-depression-self-mutilation/554917002/**
GIST	WASHINGTON — The Army issued waivers over 13 months to more than 1,000 recruits who had been diagnosed and treated for mood disorders and 95 more for self-mutilation, according to data obtained by USA TODAY. The acceptance of new soldiers with a history of serious behavioral health issues, some of which can be lifelong challenges, came as the Army struggled to meet its recruiting goals. The time period ran from Oct. 1, 2016, through Oct. 31, 2017. Last week, Army Secretary Mark Esper indicated that the Army issues waivers only for mental health issues that have been resolved or upon further review were misdiagnosed. There were no waivers issued for a history of drug overdoses or suicide attempts. “As the stigma of seeking therapy or counseling becomes less of an issue than when I grew up, you’ll see probably more cause for waivers,” Esper said. “But again, the waiver is only for an historical condition that we look at and assess. We do not allow anybody in who is undergoing therapy, who is a cutter or was a cutter, identified clearly as a cutter or is using drugs. They are not allowed into the service. And I will not accept them. Quality trumps quantity every single day of the week.” Mood disorders include conditions such as bipolar disorder and severe depression. Self-mutilation can indicate deep psychological problems. “Bipolar in most cases is a lifelong challenge,” said Elspeth Cameron Ritchie, a psychiatrist who retired from the Army as a colonel in 2010 and is an expert on waivers for military service. “It is more of a challenge when you’re younger and is not something you can simply be clear of. You’re often on medication for life.” A history of severe depression raises the risk of suicide, a problem the military sought to minimize in part by eliminating waivers for many behavioral health issues in 2009, Ritchie said. Last fall, USA TODAY reported on Army documents that showed the service tried to ease the waiver process for recruits with a history of self-mutilation, bipolar disorder and depression. The Army encountered challenging recruiting goals, including adding more than 76,000 soldiers this year. In 2017, it accepted more recruits who had fared poorly on aptitude tests, and it increased the number of waivers for marijuana use. Sen. John McCain criticized the service for accepting recruits who mutilated themselves. Figures obtained through a Freedom of Information Act request show that from Oct. 1, 2016, through Oct. 31, 2017, the active-duty Army issued waivers to 738 recruits with a history of mood disorders and 49 more with a history of self-mutilation. The Army Reserve and National Guard accepted the rest of the recruits with behavioral health issues. Soldiers with bipolar disorder often require medication such as lithium, Ritchie said. That medication must be monitored carefully, a task that may be impossible in austere combat environments far from laboratories. Manic episodes of bipolar disorder can be triggered by sleep deprivation, a common occurrence in the military, she said. She recalled treating an Army major who scrawled graffiti on walls during a “classic bipolar episode” while deployed to South Korea.

	"When you're manic, your judgment isn't good," Ritchie said. "You shouldn't be driving a tank when you're manic. You shouldn't have a rifle if you're manic." Accepting recruits with a history of behavioral health issues is risky — for the Army and the soldier, Ritchie said. "It is concerning," she said. "It can be very problematic. And we may be setting them up to fail." The Army is about 1,000 recruits behind its goal of recruits for this year.
Return to Top	

HEADLINE	**04/26 More children being diagnosed autism**
SOURCE	**http://abcnews.go.com/Health/children-diagnosed-autism-spectrum-disorder-recent-years/story?id=54762329&cid=clicksource_26_2_hero_headlines_bsq_hed**
GIST	More children are being diagnosed with autism spectrum disorder, according to new data from the Centers for Disease Control and Prevention (CDC). Their new numbers now show that autism affects one in 59 children, an increase from previously reported one in 68 children. Dr. Walter Zahorodny, a pediatrician and autism researcher, is "stunned by the speed of increase." This data was collected in 2014 through the Autism and Developmental Disabilities Monitoring (ADDM) Network, an organization described by the study's authors as "an active surveillance system that provides estimates of the prevalence of autism spectrum disorder (ASD) among children aged 8 years." In this study, the ADDM Network first identified over 10,000 children with symptoms of ASD in 11 states. A team of researchers and experts in the field then reviewed their medical and school records since birth, confirming an autism diagnosis in 5,473 children. This extremely thorough approach limited confusion and ensured accurate and consistent diagnoses and results. Part of the difficulty in autism research is that there isn't a medical "test" that determines if a child falls on the autism disorder spectrum -- it's an evaluation based on observation, so reliable numbers have been historically difficult to guarantee. The overall prevalence of autism was 16.8 per 1,000 children, or 1.68 percent, according to the study. This number varied between different states. The state with the lowest rate was Arkansas at 13.1 per 1,000 children. The state with highest rate was New Jersey at 29.3 in 1,000 children. There's no reason given for regional variation. Zahorodny, the lead researcher at the New Jersey site, states "3 percent is a real landmark, given that we started at 1 percent autism prevalence 14 years ago." These rates of autism are significantly higher than those in the last study from ADDM, which looked at a similar number of young children in 2012. This new study looked at exactly the same six locations that participated in 2012, and in these sites, the 2014 autism rates were 20 percent higher than they were in 2012. Historically, the rate of autism in white children is 20-30 percent greater than black children and 50-70 percent greater than Hispanic children. In agreement with that previous data, autism was more common in white children, although there was a significant increase in the diagnosis in black and Hispanic children, with the prevalence in white children only 7 percent greater than in black children and 22 percent greater than in Hispanic children. In agreement with past studies, autism was about four times more common in boys. One outlier: There was virtually no difference in autism rates between white, black, and Hispanic children in New Jersey. The authors argue that perhaps New Jersey's overall higher autism prevalence is related to

the more inclusive diagnosis of minority children, and therefore might be the most accurate rate in the study.

This study is not intended to be representative of the entire country. There are clear limitations, primarily because the data originated from only 11 collection sites. In addition, there were discrepancies in the amount and type of medical and educational data that was recorded from state to state. The data in this study is only as accurate as the information that was documented by physicians, counselors, and schools.

Why are more children than ever diagnosed with autism spectrum disorder?

The short answer: We don't know.

The cause of autism is still unknown. There are associations between autism and prematurity, advanced parental age, and genetics -- however no evidence of causation, according to the American Academy of Pediatrics (AAP). There's also a lot of discussion about potential environmental causes, yet again, there's no science to support these claims (the claim that vaccines cause autism has been disproven by the AAP time and time again).

To be diagnosed on the spectrum, a child must have three key characteristics: delayed language development, abnormal, repetitive behaviors, and difficulty socializing. Children with autism can have stereotypical behaviors such as rocking, spinning, hand-flapping, and toe-walking. They can also have difficulty making eye contact or playing with other children.

It's important to know that there are many children that are NOT on the spectrum who may display these behaviors. The diagnosis of autism is made by looking at a child's development, language, and behavior as a whole. If you have concerns about your child, you should speak with a pediatrician.

As the name implies, there's a wide range in severity. While many children are able to do well in school and make friends with minimal assistance, others may need significant speech and behavioral therapy to function.

Which brings us to the treatment of autism: Therapy, therapy, and more therapy.

There's no cure for autism, but certain types of therapies have been proven to improve a child's ability to function in the real world.

One of the most alarming findings in this new study is the widespread delayed diagnosis of autism. The median age of diagnosis was 52 months, just over 4 years. Children with autism should be diagnosed by 3 years old and receive appropriate therapies by 4 years old, according to Department of Health and Human Services Healthy People 2020 goals.

We are diagnosing most children too late, according to these numbers.

"We need to have strong concerted efforts toward universal autism screening," Zahorodny said in response to this data. The AAP states that all children should be screened for autism by their primary care provider at 18 months and again at 24 months.

Is autism really becoming more common?

It's unclear if this rise in autism is due to an increase in diagnosis or an increase in the actual prevalence of autism. Some scientists argue that physicians are doing a better job at diagnosing autism, particularly in minority populations, and that's why the autism numbers are up.

Thomas Frazier, the chief science officer at Autism Speaks, feels "there is a meaningful increase."

Both Frazier and Zahorodny agree that while the increase in diagnosis is contributing to the prevalence, it

	cannot be the only cause. It seems the increase in autism is significant enough that many psychologists and pediatricians worry we're missing a piece of this puzzle.
Return to Top	

HEADLINE	**04/27 China, India leaders meet amid tensions**
SOURCE	**http://abcnews.go.com/International/wireStory/china-india-leaders-meet-amid-border-tensions-54771127?**
GIST	The leaders of India and China met at a lakeside resort in central China on Friday amid tensions along their contested border and a rivalry for influence among their smaller neighbors that could determine dominance in Asia. Chinese President Xi Jinping greeted Indian Prime Minister Narendra Modi on Friday at the provincial museum in the city of Wuhan at the start of two days of talks between the heads of the world's two most populous nations. Indian media outlets, quoting unidentified top officials, reported the leaders would begin their interactions with one-on-one talks, followed by further discussions and a dinner lakeside at the resort that had been a favorite of former Chinese leader Mao Zedong. They will continue talks on Saturday with a lakeside walk, boat ride and lunch together. The countries fought a border war in 1962 and last year engaged in a 10-week standoff in the neighboring state of Bhutan. New Delhi has also been alarmed by China's moves to build strategic and economic ties with Indian Ocean nations including Sri Lanka, the Maldives and India's longtime rival Pakistan. China for its part resents India's hosting of exiled Tibetan spiritual leader, the Dalai Lama, and its control of territory Beijing says belongs to it. China claims some 90,000 square kilometers (35,000 square miles) of territory in India's northeast, while India says China occupies 38,000 square kilometers (15,000 square miles) of its territory on the Aksai Chin Plateau in the western Himalayas. Officials have met at least 20 times to discuss the competing border claims without making significant progress. Following the most protracted standoff in years, India last year agreed to pull back troops from the disputed Doklam Plateau high in the Himalayas, where Chinese troops had started constructing a road. Despite such differences, Modi hopes China can help drive Indian economic growth ahead of national elections next year. However, his administration has been reluctant to engage with Beijing's "Belt and Road" initiative linking its economies to those of Asia, the Middle East, Africa and Europe through massive loans and investments. Modi will be traveling to China again in June for a summit of the eight-member Shanghai Cooperation Organization dominated by Beijing and Moscow. Along with China, Russia and India, that group includes the Central Asian states of Kazakhstan, Kyrgyzstan, Tajikistan, Uzbekistan as well as Pakistan.
Return to Top	

HEADLINE	**04/27 India security operation targets Maoists**
SOURCE	**http://abcnews.go.com/International/wireStory/indian-security-forces-kill-maoist-rebels-54773854?**
GIST	Indian police say at least seven Maoist rebels have been killed in the second major operation by security forces against their strongholds in a week.

	Police officer Mohit Garg says security forces attacked the rebels on Friday after learning they were meeting in a forest hide-out in Bijapur district in Chhattisgarh state. He said seven rebels were killed in an exchange of gunfire. There were no immediate reports of casualties among the security forces. Last week, at least 37 Maoist rebels were killed in gunbattles between government forces and insurgents in Gadchirolia in western Maharasthra state. The Maoist rebels, who claim inspiration from Chinese revolutionary leader Mao Zedong, have been fighting India's government for more than four decades, demanding land and jobs for tenant farmers and the poor.
Return to Top	

HEADLINE	**04/26 Parkland deputies 'no confidence' w/sheriff**
SOURCE	**http://abcnews.go.com/US/florida-deputies-confidence-sheriff-presided-parkland-shooting-union/story?**
GIST	More than 500 deputies in Florida have voted that they no longer have confidence in the sheriff who presided over the Valentine's Day shooting at Marjory Stoneman Douglas High School that killed 17 students and staff. Jeff Bell, president of the Broward Sheriff's Office Deputies Association, said Thursday that out of 628 votes, 534 Broward County deputies cast a ballot to say they "no longer have confidence" in Sheriff Scott Israel. Ninety-four people voted for Israel, Bell said. The union called for the vote over sheriff's office's response to the Parkland shooting as well as Israel's response to the criticism of him in the wake of the shooting, ABC Fort Lauderdale affiliate WLPG reported. "These members have displayed great courage to come forward and vote under the threat of retaliation," Bell said. The association represents about 1,300 deputies and sergeants who "put their lives on the line every day," according to its president. Bell said it is now time for the sheriff to start listening to both members of his office as well as the leaders of Broward County. The association president took issue over Israel's leadership, policies and his handling of the budget. He also accused Israel of "taking care" of his family and friends by hiring them as "command staff at top levels" and attempting to "skirt the laws that are in place within the state of Florida." "He fails to listen to the people," Bell said. After the results of the vote were announced, Israel released a statement saying that he "will not be distracted" by the union vote. "I am accountable to the citizens of Broward County," Israel said. "My job is to continue to do the job I was elected to do, which is to ensure the safety of Broward County's 1.9 million residents." In his statement, Israel repeated a sentiment he expressed while to reporters shortly before the results of the vote were announced, which is that the vote was "designed to extort a 6.5 percent pay raise from this agency."

	Bell responded to Israel's comments by calling the sheriff a "complete liar." "This has never been abut a contract," Bell said. "This has been about his longstanding policies."
Return to Top	

HEADLINE	**04/26 NKorea Kim crosses DMZ line**
SOURCE	**http://abcnews.go.com/International/north-koreas-kim-jong-crosses-dmz-historic-meeting/story?id=54759591&cid=clicksource_4380645_1_hero_headlines_bsq_hed**
GIST	North Korean leader Kim Jong Un has crossed the line dividing the demilitarized zone to meet with South Korean President Moon Jae-in in what's being described as a historic summit. Kim made that first step, a great leap for the Korean Peninsula. The two posed for photos facing the North, then facing the South. Just about when Moon ushered Kim to walk toward the red carpet, Kim made a gesture offering Moon to take a step back across the demarcation line, to his side of the border. Whether pre-planned or not, the two smiled and took that step holding hands. Escorted by traditional music, Moon and Kim walked together to the "Peace House," a three-story building where the official summit will take place. Inside the "Peace House," Kim signed the guest book, writing in it for more than a minute. The two leaders then went into a reception room for a private conversation. It's the first time since 2007 leaders of the two countries have met and is part of a recent thawing of relations as South Korea and the United States have focused on diplomacy in their efforts to dismantle North Korea's nuclear program. The summit has been in the works for some time, with the stage being set by two previous meetings between high-level officials from the North and South, as well as the North's participation in the Winter Olympics in Pyeongchang, South Korea, earlier this year. The two nations marched under one flag.
Return to Top	

Cyber Awareness

Top of page

HEADLINE	**04/26 Mass. school district pays ransomware**
SOURCE	**http://www.telegram.com/news/20180426/leominster-pays-10k-in-bitcoin-ransom-to-undo-cyberattack-on-schools**
GIST	LEOMINSTER – The city paid $10,000 in bitcoin last week to cyber extortionists who infiltrated the school district’s computer systems over the April school break, according to city officials, affecting every school in the district. Mayor Dean J. Mazzarella called those who carried out the cyberattack “smart” and said they knew what they were doing when they gained control of the school district’s computer network. Mr. Mazzarella said he was called by the district’s superintendent, Paula Deacon, the Saturday of school vacation within 24 hours of the attack to notify him. The Federal Bureau of Investigation was notified, he said. “They (the FBI) are tracking it from here,” Mr. Mazzarella said Thursday evening. Ms. Deacon did not immediately respond to a request for a comment.

	"They were on top of their game," Mr. Mazzarella said. "They are using the best and highest technology. They were just looking for an opening and the system was hacked somehow or another." He said the $10,000 for the digital currency will come out of the city's general fund and he does not believe the incident is covered under the city's insurance. Interim Police Chief Michael Goldman said with ransomware attacks, hackers encrypt data and the only way to unlock it is with a password or by starting with a clean backup. "There is nothing the police department can do," Mr. Goldman said. "It is highly sophisticated, mostly coming from out of the country, usually Europe, and almost impossible to trace."
Return to Top	

HEADLINE	**04/27 State-sponsored hacks on Australia rise**
SOURCE	**https://www.theaustralian.com.au/national-affairs/national-security/statesponsored-cyber-attacks-on-the-rise-against-australia/news-story/1d34cc1921d15cd4f0563f7267f087b3**
GIST	State-sponsored cyber attacks targeting Australia have increased, with recent efforts allegedly carried out by Russia, Iran and North Korea making headlines either intentionally or due to poor execution, a leading cyber security expert says. Fergus Hanson, head of the International Cyber Policy Centre at the Australian Strategic Policy Institute, said those three countries, along with China, were the most common "threat actors" conducting cyber attacks around the world. "Each one has very specific motives, so if you take NotPetya (ransomware that locks a computer until a ransom is paid) … the Russians targeted that through a Ukrainian accounting firm and it was probably meant to go after Ukrainian companies," Mr Hanson said. "But because it was so poorly executed it ended up spreading from the accounting company, globally." But he said the "WannaCry" attack, that infected more than 300,000 computers and for which North Korea has been blamed, was more about demonstrating the hackers' abilities rather than purely raising money. "That was notionally a ransomware attack, but probably not specifically designed to be a money-making scheme. It was probably another capability that they were demonstrating," he said. On Wednesday computer security company McAfee released a report alleging North Korea's hacking unit had "implanted" malware into the systems of unnamed organisations in Australia and elsewhere as part of an ongoing data-theft campaign. That operation, dubbed "GhostSecret" began last month, originating in the Turkish financial sector before spreading to targets largely in the Asia-Pacific region. The federal government yesterday declined to comment on the McAfee report.
Return to Top	

HEADLINE	**04/26 Facebook criticized for 'love jihad' posts**
SOURCE	**https://www.washingtonpost.com/world/asia_pacific/a-muslim-and-a-hindu-thought-they-could-be-a-couple-then-came-the-love-jihad-hit-list/2018/04/26/257010be-2d1b-11e8-8dc9-3b51e028b845_story.html?utm_term=.f4ae12622e42**
GIST	KOLKATA, India — The 21-year-old Hindu college student was having a quiet breakfast with her mother when her phone pinged with a terrifying message. Her name was on a hit list.

She and her Muslim boyfriend had been targeted publicly on Facebook along with about 100 interfaith couples — each of them Muslim men and their Hindu girlfriends. She immediately called her boyfriend to warn him.

The Facebook post included instructions: “This is a list of girls who have become victims of love jihad. We urge all Hindu lions to find and hunt down all the men mentioned here.” At least two followers heeded the call.

The phrase “love jihad” is meant to inflame dark fears that Muslim men who woo Hindu women might be trying to convert them to Islam — a prejudice that the Hindu right has tried to stoke for nearly a decade.

But use of the term has spread on social media with the rise of the Hindu nationalist party of Prime Minister Narendra Modi, at a time when religious hatred is growing on Facebook in India, its largest market.

Facebook is facing rampant criticism that hate speech spread on the platform has fueled ethnic and religious violence in Asia, in places such as Burma and Sri Lanka.

During his appearances before Congress April 10-11, Facebook chief executive Mark Zuckerberg said the company was “working” on a way to remove hate speech within 24 hours of its appearance and adding dozens of new Burmese-language content monitors.

“It’s clear now we didn’t do enough” to prevent the platform from being “used for harm,” Zuckerberg said in his statement.

But the company has said little about its prevention efforts in India, its largest market of more than 240 million users.

The list of Hindu-Muslim couples was posted by Satish Mylavarapu, a mild-looking sales and marketing manager in Bangalore who propagates militant Hinduism to thousands of followers in Facebook groups and elsewhere.

“It’s a matter of Muslims taking over our blood and taking over our wombs — the wombs that would give Hindu children,” he said.

Highly motivated Hindu extremist “volunteers” across India assembled the list by meticulously plotting the locations of mosques and girls schools and colleges around the country and combing young women’s profiles for photos or posts that would link them with Muslim men.

Meanwhile, conservative Hindu groups supporting Modi’s powerful Bharatiya Janata Party began pushing into areas in India’s east and south traditionally dominated by other languages and regional parties, including the couple’s home state of West Bengal.

In recent weeks, West Bengal has been roiled by riots between Hindus and Muslims that followed sword-waving devotees marching in honor of Lord Ram — a Hindu deity who is not normally worshiped in the region. At least four people died.

Civil society groups have charged that Facebook has not acted quickly enough in such instances to curb the hate speech that inflamed tensions throughout Asia, including Muslim-Buddhist riots in Sri Lanka and Burma’s exodus of more than 850,000 Rohingya Muslims into Bangladesh. Facebook was dubbed the “beast” in that crisis by a United Nations monitor.

In India, a March study by the Observer Research Foundation, a think tank based in New Delhi, showed that religion is increasingly used as a basis of hate speech on Facebook, a jump of 19 to 30 percent between 2016 and 2017.

	"I don't think Facebook has a clue how to monitor hate speech," said Maya Mirchandani, a senior fellow who co-wrote the study. She said that more proactive text monitoring systems are not in place, including among its rapidly growing non-English speaking audiences. "Maintaining a safe community for people to connect and share on Facebook is absolutely critical to us," a Facebook spokesman said in a statement. "We have policies that prohibit hate speech and credible threats of harm, and we will remove this content when we're made aware of it."
Return to Top	

HEADLINE	**04/27 Chrome VPN extensions leaking data**
SOURCE	**https://www.hackread.com/chrome-vpn-extensions-leaking-your-dns-data/**
GIST	Last month, HackRead reported how tons of popular VPN (Virtual Private Network) software were leaking real IP addresses of users through WebRTC leak along with a list of VPN vendors saving users' Internet logs despite claiming otherwise. Now, a new study has been conducted according to which some popular Chrome VPN extensions are leaking DNS related data of their users – Here, it must be noted that the DNS leak is not related to the WebRTC issue but DNS prefetching in Chrome browser activated by default. The study was conducted by John Mason of TheBestVPN alongside with an ethical hacker from Cure53 who goes by the Twitter handle of File Descriptor. It may shock many that 7 out of 17 VPN extensions on Chrome are leaking DNS data. Chrome VPN Extensions that are leaking DNS 1: Hola VPN 2: Touch VPN 3: Betternet 4: DotVPN 5: HoxxVPN 6: Ivacy VPN 7: Opera VPN The aforementioned VPN extensions are used by millions of users around the world, for instance, Hola VPN has over 8.7 million users, Touch VPN has 2 million users, Betternet is used by 1.4 million users while DotVPN has 900,000 users. This means DNS related data of millions of users is currently at risk. Chrome VPN Extensions that are NOT leaking DNS 1: NordVPN 2: PureVPN 3: WindScribe 4: CyberGhost 5: TunnelBear 6: ZenmateVPN 7: HotSpot Shield 8: VPN Unlimited 9: Avira Phantom VPN 10: Private Internet Access
Return to Top	

HEADLINE	**04/26 Sounds of DDoS in NetFlow logs**

SOURCE	**https://www.infosecurity-magazine.com/news/cadence-in-chaos-sounds-of-ddos-in/**
GIST	For those who appreciate the healing power of music, new research could prove to be a magical security tool. By correlating traffic types from NetFlow logs with sounds of instruments, researchers at Imperva were able to translate changes in network traffic into song. Inspired by a TED Talk called "Can We Create New Senses for Humans?" presented by Dr. David Eagleman, adjunct professor in the Department of Psychiatry & Behavioral Sciences at Stanford University, Imperva's team wondered whether tapping into the sense of sound could change the way they interpret network traffic. "Auditory perception, we learned, has a lot of advantages oversight, especially in terms of processing spatial, temporal and volumetric information. The ability to register the most delicate differences in frequency resolution and amplitude opens up a Pandora's Box worth of possibilities in data perception," Imperva wrote in a blog post. Turns out that sonification is an effective monitoring tool, so they set to work to figure out how to make the internet sing. In order to collect NetFlow data, they created a Python 3 script, then processed the data into Open Source Control messages which were then converted into sound using a Ruby-based algorithmic synthesizer. Assigning different instrumental sounds to the varied traffic types created a melody that revealed the ebb and flow of the traffic levels and also revealed shifts in pitch and volume. A significant shift in traffic would be the harbinger of a DDoS attack. So as not to rely solely on shifts in volume as an alert, the team decided to add an additional mechanism that would really sound an alarm bell and activate a mitigation service. Their choice? The sound of a tomato being squeezed.
Return to Top	*Click on source link to hear sonorous sounds of data*

HEADLINE	**04/26 For sale: next-generation phishing kit**
SOURCE	**https://www.scmagazine.com/simple-but-not-cheap-phishing-kit-found-for-sale-on-dark-web/article/761520/**
GIST	Cybercriminals are nothing if not attuned to finding new customers for their wares, as Check Point and CyberInt found when they came across a next-generation phishing kit for sale on the Dark Web geared toward the neophyte, but discerning, hacker. A joint investigative venture by Check Point and CyberInt found [A]pache Next Generation Advanced Phishing Kit on the Dark Web, which the companies described as a fifth-generation level kit. The kit is not necessarily inexpensive retailing for between $100 and $300, compared to the $20 or $50 most kits sell for, but for the price [A]pache delivers what the researchers called one of the most advanced phishing kits yet spotted. "With [A]pache's next-generation phishing kit, however, threat actors are provided with a full suite of tools to carry out their attack. These include an entire back-office interface with which they can create convincing fake retail product pages and manage their campaign," the report stated. This includes having their own versions of sites including, Walmart, Americanas, Ponto Frio, Casas Bahia, Submarino, Shoptime and Extra. At this point, the product is developed primarily for use in the Brazilian market, but the fact that some American brands are also included means it could be used in the U.S. too. The kits then lay out the step by step process the users need to follow to get their phishing scam up and running. After choosing a retailer to emulate the customer are shown how to register a domain name to be used, a

	payment option for the victims is picked. Next the malicious actor inserts legitimate product URLs from the site being replicated to help make the fake site appear real. This includes setting prices for the products and the kit sellers suggest making the prices competitive with what is available in the real world to add an extra layer of authenticity. “Care needs to be taken here though as reducing prices too low though would raise suspicions with captivated ‘customers'. Finally, the kit owner has to learn how to view the victim's stolen information,” the report states.
Return to Top	

HEADLINE	**04/26 Hackers love healthcare**
SOURCE	**http://www.darkreading.com/endpoint/why-hackers-love-healthcare/a/d-id/1331537**
GIST	Much like the rest of the world, healthcare organizations are shifting work to cloud services in order to improve accessibility and patient care. However, the migration of these workloads and moving valuable information such as PHI (personal health information) and PII (personally identifiable information) to the cloud has also led to cybercriminals taking a particular interest in the industry. The number of ransomware and other malware attacks is rising incredibly fast in the healthcare industry, putting human lives as well as critical data at risk. From 2011 through 2014, the sector — including hospitals, labs, pharmacies, drug companies and outpatient clinics — experienced the highest number of data breaches of all industries. What makes these organizations such a popular target? **1. Highly Valuable Data** One of the key aspects making healthcare organizations a top target is the value of their data. Commonly, a single stolen credit card number yields an average $2,000 profit and quickly becomes worthless. Healthcare data, however, such as PHI or PII, is extremely valuable on the black market. A single PHI file, for example, can yield a profit of up to $20,000. This is mainly because it can take weeks or months for a healthcare data breach to be discovered, enabling cybercriminals to extract much more valuable data. Moreover, because healthcare data can contain dates of birth and Social Security numbers, it is much more difficult or even impossible to change, so thieves can take advantage of it for a longer period of time. **2. Lack of IT Investment and Training** Another reason the healthcare industry is popular among cybercriminals is its systematic underinvestment in IT security. Most healthcare organizations spend just 3% of their IT budgets on security, while the SANS Institute — the largest provider of cybersecurity training and certifications — recommends spending at least 10%. For most healthcare organizations, security is often an afterthought. They don't provide regular cybersecurity training for their employees, which could help reduce insider threats. For example, 18% of healthcare employees say they're willing to sell their login credentials for between $500 and $1,000. And about one-quarter of healthcare employees know someone in their organization who has engaged in this practice. To address employee-related cyber vulnerabilities, it's important to note that while training is essential, it won't magically protect patients’ digital data. Although some hospitals struggle to deploy the most basic IT security measures, such as intrusion detection and the ability to wipe lost or stolen devices, it is imperative that basic cyber hygiene practices are coupled with ongoing training to both protect well-intended employees and mitigate future data loss from those seeking to profit. **3. Highly Connected Systems** Having shifted workloads to the cloud, healthcare organizations have highly connected systems that run the risk of being deeply affected even if the attack takes place on smaller, partial systems. In other words,

	a cyberattack in one place could bring down the entire system. In May 2017, the WannaCry ransomware attack forced multiple hospitals across the United Kingdom to turn away ambulances transporting patients and cancel surgeries that were within minutes of starting. Even basic processes like admitting patients and printing wrist bands were compromised. The impact of WannaCry illustrates how important it is for healthcare organizations to be able to function and provide patient care during a cyberattack. After all, lives are at risk, meaning there's a general urgency to get back to business as soon as possible. For attackers, this urgency makes it extra tempting to target healthcare organizations, because they assume it will make them more likely to pay the ransom to reverse the infection.
Return to Top	

HEADLINE	**04/26 New phishing attack uses online quiz**
SOURCE	**http://www.darkreading.com/vulnerabilities---threats/new-phishing-attack-targets-550m-email-users-worldwide/d/d-id/1331654**
GIST	A new phishing campaign was discovered sending more than 550 million emails within the first quarter of 2018, according to data from Vade Secure. The threat was discovered in early January and has primarily hit users in the US, UK, France, Germany, and the Netherlands. Victims receive emails disguised to come from popular brands and services in their home country. Attackers try to steal their banking information by offering coupons or discounts in exchange for their participation in an online quiz or contest. Experts believe a serious criminal organization is behind this campaign, which doesn't use pirated websites as many phishing attacks do. This one appears to use leased and legitimate IP addresses, servers, and domain names, which would drive infrastructure costs up to tens of thousands of dollars. They also use tools to shorten URLs and conceal the ultimate destination. These sophisticated techniques caused the threat to bypass many existing email security tools, researchers report.
Return to Top	

HEADLINE	**04/26 Phishing campaign delivers new malware**
SOURCE	**https://www.zdnet.com/article/ransomware-warning-this-phishing-campaign-delivers-new-malware-variants/**
GIST	A new spam campaign designed to infect victims with GandCrab ransomware has surged over the past few days, as the criminals behind the scheme look to infect as many victims as possible. GandCrab first emerged in January and those behind it have regularly updated the ransomware and altered their attack techniques in order to maximise profit from the file-encrypting malware. Analysis by researchers at security company Fortinet found that three new samples of GandCrab 2.1 are being distributed as the payload in a single mass spam campaign. "This means that newly created samples are being pushed simultaneously, possibly with different configurations, or simply in an attempt to evade specific file signatures," said researchers. Phishing emails feature common subjects about about payments, tickets, invoices and orders and contain a Javascript attachment which when executed, downloads GandCrab from a malicious URL. Tens of thousands of GandCrab spam emails are being distributed each day, with mail servers hosted in the US by far the most common target, accounting for three quarters of deliveries. When it comes to

	successful infections, the US currently accounts for the fourth largest percentage of victims, behind Peru, Chile and India. Those infected with GandCrab are directed to a site which can only be accessed by the Tor browser, where they can "purchase" a private key to decrypt the files. A ransom note demands a payment of $400 - which previous GandCrab attacks have demanded be paid in Dash cryptocurrency, which is faster to process and more difficult for the authorities to track than Bitcoin.The figure is doubled if the victim doesn't pay within a certain amount of time.
Return to Top	

HEADLINE	**04/26 Dutch police shutter Anon-IB**
SOURCE	**https://www.bleepingcomputer.com/news/security/police-shut-down-anon-ib-an-infamous-revenge-porn-forum/**
GIST	Dutch police announced today that they had seized the servers of Anon-IB, a notorious online portal where users would share pictures of revenge porn and child pornography. The website became famous after it hosted pictures from the Celebgate (Fappening) scandal, nude photos of US female marines, photos of underage girls from US high-schools, and was the go-to place were angry boyfriends or girlfriends would go to upload nude photos of their ex-partners —a practice known as revenge porn. Anon-IB is also famous for its "collectors" —users who keep private nude photo collections, which they trade with each other like baseball or Pokemon cards. Anon-IB servers were located in the Netherlands Besides shutting down the site, Dutch police also announced the arrest of three suspects — a 28-year-old from the city of Heerlen, a 31-year-old from Culemborg, and a 35-year-old from Groningen. They are also currently investigating two other suspects, a 19-year-old from Terneuzen, and a 26-year-old from Geleen. These five are regular users who uploaded pictures on the site, not Anon-IB administrators. Police arrested the three after seizing Anon-IB servers located in the Netherlands. They tracked down the five because the suspects failed to hide their IP addresses. Police told Dutch TV station RTL Nieuws that some of the suspects they are investigating would meet women on the street, get their names, and then try to guess their passwords by for their online accounts, hoping to discover nude images or videos. The suspects said they combined names, birthdays, and other common strings when trying to guess a victim's account password. Besides storing nude photos, the forum also hosted tutorials on hacking online accounts. Entire threads would teach readers how to obtain publicly leaked data, extract the passwords from public breaches, and use the passwords to hack into people's online accounts to search for nude photos. RTL Nieuws journalists also found topics where Anon-IB users would talk about extorting hacked victims, either for cryptocurrency or for more nude photos to add to their collections. Dutch police to notify all affected victims Dutch police say they already notified some of the women who had their data leaked on the site and plan to contact further victims if they manage to identify more persons in the coming months. Police said that many of the women's whose data was uploaded on the site were unaware they'd been hacked.

Return to Top	

HEADLINE	**04/26 New 'interesting' C# ransomware emerges**
SOURCE	**https://www.bleepingcomputer.com/news/security/new-c-ransomware-compiles-itself-at-runtime/**
GIST	A new in-development ransomware was discovered that has an interesting characteristic. Instead of the distributed executable performing the ransomware functionality, the executables compiles an embedded encrypted C# program at runtime and launches it directly into memory. Discovered by MalwareHunterTeam, this ransomware contains an encrypted string that is embedded into the dropper…This string is then decrypted using an included decryption key. Now that the source code for the ransomware executable has been decrypted, the decrypted code is sent to another function that compiles it using the CSharpCodeProvider class and launches it directly into memory. This method is probably being used to prevent the dropper from being detected by security software as any malicious behavior is hidden inside the encrypted string. As for the ransomware itself, other than it saving the decryption key and IV to a file on the desktop, it is fully functional. Therefore, it wouldn't be surprising to see the ransomware being distributed at some point.
Return to Top	

HEADLINE	**04/26 MongoDB server exposes Bezop users**
SOURCE	**https://www.bleepingcomputer.com/news/security/exposed-mongodb-server-exposes-details-of-cryptocurrency-users/**
GIST	Security researchers have stumbled across a MongoDB database containing the personal details of over 25,000 users who invested in or received Bezop (BEZ) cryptocurrency. According to cybersecurity firm Kromtech, the database contained information such as full names, home addresses, email addresses, encrypted passwords, wallet information, and scanned passports, driver's licenses, or IDs. The database stored information related to a "bounty programme" that the Bezop team ran at the start of the year, during which it handed out Bezop tokens to users who promoted the currency on their social media accounts. A Bezop spokesperson admitted to the breach, claiming the database was inadvertently exposed online while the dev team dealt with a DDoS attack on January 8. A spokesperson told Bleeping Computer today that no user funds were stolen following this exposure. Database is now secured The Bezop spokesperson said the database contained details on around 6,500 ICO investors, while the rest was for users who participated in the public bounty program and received Bezop tokens in return. The data appears to have remained exposed online until March 30, when Kromtech researchers spotted the MongoDB database on a Google Cloud server. The database was without an authentication system in place, allowing anyone connecting to it access to the stored information. Kromtech researcher Bob Diachenko told Bleeping Computer today that the database was taken down within hours after he tweeted the Bezop team.

	"That database has since been closed and secured," the Bezop team said this week, also claiming it notified users of the incident already. "Investor identity cards were also not stored on the database rather a URL link to them. This is also offline now." Diachenko confirmed that an authentication system now protects the database he found at the end of March, albeit there is no way of telling if anyone except the Kromtech team discovered the same database.
Return to Top	

HEADLINE	**04/26 NKorea elites ditching Facebook**
SOURCE	**https://www.bleepingcomputer.com/news/technology/north-koreas-elites-are-ditching-facebook-for-chinese-social-networks/**
GIST	Following the publication of a report in July 2017, North Korea's elites, some of the country's few citizens allowed on the Internet, have greatly altered their online behavior, and are now obfuscating their browsing activity, and have ditched US websites like Facebook or Instagram for alternative Chinese social networks. The company at the base of these findings is US threat intelligence firm Recorded Future. The company's engineers have been passively tracking and analyzing Internet traffic from North Koreans inside and outside the country's borders since April 2017. They published an initial report last summer, highlighting how the very few North Koreans that were allowed to surf the world wide web were no different than any other user. The report showed that North Koreans liked to spend most of their time streaming videos, playing games, interacting on social networks, or watching porn. North Koreans are now Tor and VPN fans But the report appears to have made it into the North Korean government's hands as well, because, between December 2017 and March 2018, the same researchers spotted a major shift in online behavior. The biggest change was that the amount of obfuscated traffic has grown from 1 percent in July 2017 to nearly 13 percent in March this year. Obfuscated traffic is web activity hidden behind encrypted HTTPS connections, under Tor clients, or VPN, VPS, or other tunneling protocols (known as PPTPs). Popular web obfuscation protocols in North Korea There was a clear indication that those very few North Koreans allowed to surf the Internet were clearly told to hide their activity whenever possible. North Koreans ditch Facebook Furthermore, authorities appear to have also instructed users to stop hanging around on US social networks. Nowadays, North Koreans are avid users of Alibaba, Tencent, and Baidu. "In July, our data demonstrated that North Korean leadership heavily consumed Western social media, especially Facebook, Google, and Instagram," says Recorded Future analyst Priscilla Moriuchi. "In fact, Facebook was by far the most popular service, with more than double the daily actual usage than any of its Chinese-language counterparts." Nowadays, things have dramatically changed, so much so that Facebook and Instagram activity had diminished so much, it wasn't even visible on a Recorded Future chart.
Return to Top	

HEADLINE	**04/27 World largest spam botnet gets update**
SOURCE	**https://www.bleepingcomputer.com/news/security/worlds-largest-spam-botnet-finds-a-new-way-to-avoid-detection-for-now/**
GIST	Necurs, the world's largest spam botnet, with millions of infected computers under its control, has updated its arsenal and is currently utilizing a new technique to infect victims. This new technique consists of sending an email to a potential victim containing an archive file, which unzips to a file with the extension of .URL. This is a typical Windows shortcut file that opens a web page directly into a browser, instead of a location on disk. The final destination of this link is a remote script file that downloads and automatically executes a final payload. Necurs dropping Quant Loader via .URL shortcut files For this particular spam run, Necurs had been infecting victims with Quant Loader, a run-of-the-mill and nothing-special malware family that is intended only to gain boot persistence and download another strain of more potent malware down the road. While this technique is most likely not new entirely, as crooks have abused .URL files in the past, it is new for Necurs. What makes this technique stand out is the simplified infection chain, which now relies only on delivering a zipped .URL shortcut file. For the past six years, since Necurs has been around, the botnet's operators have rarely used such a simple spam technique and have always relied on complicated infection chains. We've seen stuff like one-time or double-zipped archives delivering WSF files, JS files, Visual Basic scripts, and all sorts of Office file formats, either boobytrapped with macros or leveraging exploits to infect victims. New technique evades email malware scanners The purpose of this much simpler routine is to avoid malware scanners that analyze emails, looking for malicious links or boobytrapped attachments. Such solutions work on preset rules, many of which have been set up by security researchers based on previously observed malicious patterns. The deployment of a simple .URL file is not a game-breaker, as security researchers only need to update existing detection rules with a new one, but this will give the Necurs botnet time to breathe and infect victims easier in the following weeks, as email malware scanners will receive updated detection rules. At that point, just like we've seen Necurs in the past years, botnet operators will just make a small tweak to the infection chain —like putting the .URL file inside a double-zipped file instead of a one-time zipped file— and this whole cat and mouse game will start anew. How users can protect themselves What users need to know —or remember, if they're old enough to have seen this trick before— is that .URL files work like typical Windows shortcut file, such as .LNK, and hence, can use custom icons. Trend Micro, the cyber-security firm who spotted this recent Necurs .URL-based malspam campaign, warns that crooks are using the standard folder icon to hide .URL files. This makes it somewhat easy to trick users into thinking the email file attachment they just unzipped has created a folder that they need to enter and view the actual file. Unfortunately, this is what crooks want because trying to access this faux folder will launch the infection chain.
Return to	

Top

HEADLINE	**04/26 Crypto crime wave is here**
SOURCE	**https://www.wsj.com/articles/the-crypto-crime-wave-is-here-1524753366**
GIST	On a Saturday afternoon in November, Louis Meza made plans to meet a friend and fellow cryptocurrency enthusiast for drinks at Ruby Tuesday in New York City's Times Square. "We're going to have a great time," Meza said in a text. "And by the way, I'm putting you in an Uber car at the end of the night." A former salesman at the food-delivery service Grubhub, Meza is described by friends as gregarious and courteous—a 35-year-old poker buff with an entrepreneurial streak and an appetite for risk. The two men had known each other for about 15 years. They met for drinks and, around 7:40 p.m., Meza's friend said he was heading to the subway. Meza insisted on an Uber and ushered his friend—listed in court documents as "the victim"—into a gray minivan waiting outside. According to the Manhattan district attorney's office, a gunman hiding in the back seat of the van popped up and demanded the victim's wallet, keys, cellphone and a USB drive, which contained ether, a type of cryptocurrency. The victim handed over everything but the drive, which wasn't on his person; the gunman pulled a hood over the victim's head. "Where is your 24-word passphrase?" he demanded again and again. After two hours, the victim managed to escape. He found himself in Harlem, where, according to prosecutors, he called 911 from a deli. The victim had made a "very small investment" in cryptocurrency as early as 2010 that had since mushroomed to $1.8 million. He kept the ether on a USB drive in his apartment, along with a piece of paper containing the passphrase required to access it. By the time he got home, both the drive and the passphrase were gone. An indictment unsealed in December accuses Meza of robbery, kidnapping and other crimes. Meza pleaded not guilty. But according to prosecutors, security-camera video shows Meza unlocking the victim's apartment with keys and emerging about a minute later with a small white box, which, according to the victim, held his ether. The day after the theft, Meza transferred $1.8 million in ether to an online account in his own name. "We see the $1.8 million get deposited into that account on the morning of November 5, and then we see it being moved all over the place," Assistant District Attorney James Vinocur told the judge in the case. Vinocur told the judge that prosecutors had been able to seize only about $600,000 of the money. "$1.2 million is still outstanding, and we don't know where it is," he said. "That is the nature of cryptocurrency, that we can see the address it was sent to. It doesn't mean much to us. It's just a string of numbers and letters." And what seemed like an open-and-shut robbery case is proving much more complicated. The Meza case is part of a recent spike in cryptocurrency crime, prompted by the soaring values of digital currencies like bitcoin. Chainalysis Inc., a firm that analyzes cryptocurrency transactions, says reported thefts of bitcoin worldwide increased from $3 million in 2013 to $89 million last year. For many criminals, cryptocurrency is less cumbersome than cash. Hackers hold computer systems hostage and demand instant, anonymous payment in bitcoin. Drug dealers sell in dark corners of the internet, obscuring their names and locations. Narcotics traffickers move and launder their profits with clicks of a mouse. "The cases have exploded," says Gabriel Bewley, a special agent in the virtual-currency initiative at the Drug Enforcement Administration. Blockchain Intelligence Group Inc., which makes software that tracks cryptocurrency use, estimates illegal activity accounts for about 20% of the transactions of five major cryptocurrencies—bitcoin, Monero, Zcash, ether and litecoin—or about $600 million each day. Researchers working at the University of Sydney used artificial intelligence to identify cryptocurrency transactions consistent with criminal behavior and estimated $72 billion of illegal activity last year using bitcoin alone.

What exactly is cryptocurrency?
In the wake of the 2008 financial crisis, bitcoin's anonymous creator published a white paper under the pseudonym Satoshi Nakamoto. "Bitcoin: A Peer-to-Peer Electronic Cash System" described the major impetus behind the digital currency: Eliminate the need for third-party financial institutions like banks and brokerages. "A purely peer-to-peer version of electronic cash," Nakamoto wrote, "would allow online payments to be sent directly from one party to another."

Every bitcoin transaction would be recorded on an encrypted public ledger now known as the blockchain, preventing someone from spending the same bitcoin twice or counterfeiting the currency. And because the blockchain is stored on a decentralized network of computers, the records of these transactions would be theoretically impossible for hackers to corrupt. But removing banks from the equation poses a problem for law enforcement, which relies on financial institutions to provide records needed to secure convictions.

Bitcoin is one of about 1,500 cryptocurrencies, all of which exist in a legal and regulatory gray area. The Internal Revenue Service treats cryptocurrency like property—not like a currency or a security but like an asset. The Securities and Exchange Commission, meanwhile, has said that initial coin offerings, or sales of new cryptocurrencies, should be subject to securities laws to protect investors from fraud. In the court system, the definition is similarly ambiguous.

A federal judge in Brooklyn is expected to rule on one issue in the coming months. The case involves a Brooklyn businessman named Maksim Zaslavskiy who, in July and September, launched initial coin offerings for two new cryptocurrencies: REcoin, purportedly backed by real estate, and Diamond Reserve Coin, supposedly backed by diamonds. Federal prosecutors charged Zaslavskiy with fraud, arguing that he sold unregistered securities. Zaslavskiy's lawyers have asked the judge to dismiss the charges, arguing that cryptocurrencies aren't securities and therefore aren't subject to securities laws. "Virtual currencies such as the ones at issue here present regulatory challenges for securities laws that were written in the 1930s—decades before the invention of the computer," the lawyers, Mildred Whalen and Len Kamdang, wrote in February. Zaslavskiy's case is pending.

In 2014, Florida state prosecutors charged website designer Michell Espinoza with money laundering after he sold bitcoin to an undercover detective who said he would use the currency to buy stolen credit-card numbers. Espinoza, prosecutors argued, was acting as an unlicensed money-services business and facilitating illegal activity. The judge disagreed. "This Court isn't an expert in economics," she wrote. "However, it is very clear, even to someone with limited knowledge in the area, that bitcoin has a long way to go before it is the equivalent of money." Prosecutors have appealed the ruling.

This legal uncertainty, combined with cryptocurrencies' volatility, is complicating the prosecution of Louis Meza. The Manhattan district attorney's office asked to sell the seized ether because prosecutors feared its value would decrease, says Moshe Horn, Meza's lawyer.

"They wanted to turn it into cash so they couldn't be blamed," Horn says. "Then the question becomes, do they have a right to?"

The district attorney's office ultimately decided not to sell it. The answer to his lawyer's question is still unclear.

Digital currency's criminal history
Criminal activity has plagued digital currency since its inception. "Remember E-gold?" says Serrin Turner, a cybersecurity lawyer in New York. E-gold was the name of both a digital-currency service and a currency that was purportedly backed by actual gold. Its founder designed it as a payment system that would allow for the easy, anonymous transfer of funds. This made it popular with criminals, according to federal prosecutors, who claimed E-gold facilitated child exploitation, investment scams and other criminal activities. In 2008, E-gold's directors pleaded guilty to money-laundering charges. The service subsequently closed, but similar payment systems quickly took its place.

"This notion has been around for a long time," Turner says. "Digital currency has greased the wheels of

the cybercriminal ecosystem."

Before joining the firm Latham & Watkins, Turner was a prosecutor in the U.S. attorney's office in Manhattan, where he prosecuted E-gold successor Liberty Reserve, a Costa Rica-based digital-currency business that enabled anonymous payments. In 2016, Liberty Reserve founder Arthur Budovsky admitted to laundering more than $250 million in criminal proceeds and was sentenced to 20 years in prison.

Crime involving digital currencies has skyrocketed in lockstep with their valuations. From bitcoin stickups to global money laundering, tech-savvy criminals are becoming increasingly anonymous. And law enforcement is scrambling to keep up.

Turner's best-known case, the one that put bitcoin on the map, was the prosecution of the founder of Silk Road, the first large-scale "darknet" market to use cryptocurrency. Darknet markets exist on the so-called Dark Web, a section of the internet accessible only with software designed to make users anonymous. Silk Road was an online marketplace that accepted only bitcoin as payment, allowing its vendors and customers to conceal their locations and identities. From 2011 to 2013, more than 100,000 Silk Road users bought and sold over $200 million in drugs and illegal goods, ranging from weapons to forged driver's licenses, according to prosecutors.

Authorities closed Silk Road in October 2013. Silk Road 2.0 appeared the next month and remained active for about a year before authorities shut it down. Other illicit marketplaces emerged to take its place. The July 2017 takedown of the darknet market AlphaBay involved the cooperation of law-enforcement agencies in more than seven countries. According to the Federal Bureau of Investigation, the site had twice as many users as Silk Road, and from 2015 to 2017, transactions totaled more than $1 billion in bitcoin and other digital currencies.

Headline-grabbing arrests and seizures have done little to slow the flow of money to darknet markets. Last year, $660 million in bitcoin was sent to darknet marketplaces, up from $57 million in 2012, according to Chainalysis.

"It's kind of like Whac-A-Mole," says Greg Cipolaro, the chief executive of Digital Asset Research, a cryptocurrency-analysis firm. "Every time they close one down, another one opens."

One of the largest darknet marketplaces operating today is Dream Market, where, on a recent afternoon, Turkish heroin was advertised as "topquality!" and "Vanilla Kush weed" as "100% organic." There were weapons for sale—tasers, butterfly knives, a "wallet ninja multi-tool"—along with Nike tracksuits and "lifetime" porn-account subscriptions. A vendor named Bizzey advertised "5x XTC 220mg Donald Trump," for 0.004038 bitcoin, or $31.68. A photo showed orange tablets resembling children's multivitamins in the shape of Donald Trump's head. Bizzey had 4.94 stars and 36 reviews. "Amazing speed and stealth," read a five-star review. "Even got a freebie. would recommend!"

In December, officers led Louis Meza into a Manhattan courtroom, where a clerk informed him that he had been charged with grand larceny, kidnapping, robbery and other crimes. The clerk asked Meza how he would like to plead.

"Not guilty," Meza said.

During the hearing, Vinocur, the assistant district attorney, said the prosecution's case was strong, citing the security-camera video and statements Meza made to police.

According to Meza's lawyer, the case will be uncommonly difficult for the prosecutors. "The burden of proof is on the prosecution to show where the cryptocurrency is, how did it get there and who put it there," Horn says. "It's not like walking into a bank vault and saying, 'There's the cash.' "

The missing ether underscores a larger issue facing law enforcement: the difficulty—and occasionally the impossibility—of investigating and prosecuting crimes involving cryptocurrency. "Prosecutors are always

about following the money," says Scott Christie, a white-collar criminal-defense lawyer at McCarter & English, who previously headed the computer-hacking division at the U.S. attorney's office in New Jersey. "If you can't follow the money, you can't prove your case."

A number of firms have developed software designed to follow the flow of cryptocurrency transactions. In a financial-technology co-working space in Manhattan, Kim Grauer, a senior economist at Chainalysis, opens a software program called Reactor. "When you go into Reactor, you're going into the world of bitcoin," Grauer says. Reactor and other so-called blockchain-analysis programs visually depict the trail of cryptocurrency transactions, allowing law enforcement to see the movement of funds in a way that would be impossible with cash. But these programs have their limits. Many transactions are associated only with anonymous addresses, represented by the "string of numbers and letters" that confounded prosecutors in the Meza case.

To identify an individual associated with one of these addresses, Grauer says, an investigator would look for an "off ramp," the point where cryptocurrency is converted into fiat, or government-backed, currency. This is typically done through exchanges, websites that let users trade cryptocurrencies and convert them to traditional currency.

Exchanges are the part of the cryptocurrency ecosystem most accessible to law enforcement. If a criminal uses an exchange that collects its customers' personal information, prosecutors can attach a name to a transaction—provided the exchange cooperates with authorities. But tech-savvy criminals are increasingly opening accounts with fake names at overseas exchanges that don't comply with U.S. laws.

In June, Kathryn Rodriguez, a former assistant U.S. attorney at the Justice Department in Washington, testified about cryptocurrency in front of a U.S. House of Representatives committee. Rodriguez said subpoenas are ineffective when exchanges don't require names or identifying documents to open an account. "Even though investigators can follow the funds by analyzing the blockchain, they may not be able to connect those funds to a culprit in the real world," she said. "We have received 'Mickey Mouse' who resides at '123 Main Street' in subpoena returns."

Noncompliant exchanges are just one of the tools criminals use to evade authorities. "What we're seeing crooks do now is use a mixer or a tumbler," says Tom Flattery, a deputy district attorney in the high-tech unit of Santa Clara County's district attorney's office. "It's a service that will mix transactions with several others, moving through multiple accounts and multiple countries. There's no way for law enforcement to track it."

One cryptocurrency mixer, Bitcoin Blender, claims to make transactions "100% anonymous." According to the company's website, "Bitcoin Blender completely removes any connection you have with the coins you buy or sell, meaning nobody can use Blockchain Analysis to track you down." Unsurprisingly, Bitcoin Blender could not be reached for comment.

Criminals seeking additional protection have abandoned bitcoin in favor of currencies that offer additional privacy protections. Monero, a currency its website calls "secure" and "untraceable," uses technology that hides the sender, receiver and amount of transactions. Although recent research has pointed to possible security flaws, a Monero spokesman has said developers have made improvements designed to increase privacy.

Mixers and identity-shielding currencies point to a future where criminals' financial transactions could be impossible to trace. Large narcotics traffickers and money launderers are hiring increasingly sophisticated technicians to move cryptocurrencies as discreetly as possible, says Jean Walsh, chief of the investigations division at the Bronx district attorney's office, a trend she expects to continue until cryptocurrency is adequately regulated. "The amount of effort to evade being traced and tracked, both on computers and on electronic transactions—it's something they spend 24 hours a day concentrating on," Walsh says. "Once the criminals continue to improve their technology, our fear is that they will be anonymous."

Return to Top

HEADLINE	**04/26 Study: non-malware attacks on the rise**
SOURCE	**http://www.infosecisland.com/blogview/25059-Non-Malware-Attacks-What-They-Are-and-How-to-Protect-Against-Them.html**
GIST	Non-malware attacks are on the rise. According to a study by the Ponemon Institute, 29 percent of the attacks organizations faced in 2017 were fileless. And in 2018, this number may increase up to 35 percent. So, what are non-malware attacks, how do they differ from traditional threats, why are they so dangerous, and what can you do to prevent them? **Non-malware attacks: what are they?** Non-malware or fileless attack is a type of cyber attack in which the malicious code has no body in the file system. In contrast to the attacks carried out with the help of traditional malicious software, non-malware attacks don't require installing any software on a victim's machine. Basically, hackers have found a way to turn Windows against itself and carry out fileless attacks using built-in Windows tools. The idea behind non-malware attacks is pretty simple: instead of dropping custom tools that could be flagged as malware, hackers use the tools that already exist on a device, take over a legitimate system process and run the malicious code in its memory space. This approach is also called "living off the land." This is how a non-malware attack usually happens: • A user opens an infected email or visits an infected website • An exploit kit scans the computer for vulnerabilities and uses them for inserting malicious code into one of Windows system administration tools • Fileless malware runs its payload in an available DLL and starts the attack in the memory, hiding within a legitimate Windows process Fileless malware can be downloaded from an infected website or email, introduced as malicious code from an infected application, or even distributed within a zero-day vulnerability. **Why are non-malware attacks so dangerous?** One of the main challenges posed by fileless malware is that it doesn't use a traditional malware and, therefore, doesn't have any signatures that an anti-malware software could use to detect it. Thus, detecting fileless attacks is extremely challenging. To understand better why they pose so much danger, let's take a look at some of the most recent examples of fileless attacks. One of the first examples of fileless malware were **Terminate-Stay-Resident (TSR)** viruses. TSR viruses had a body from which they started, but once the malicious code was loaded to the memory, the executable file could be deleted. Malware that uses vulnerabilities in such scripts as JavaScript or PowerShell is also considered to be fileless. Even the much-talked-of ransomware attacks WannaCry and NotPetya used fileless techniques as a part of their kill chains. Another example of a non-malware attack is the UIWIX threat. Just like WannaCry and Petya, UIWIX uses the EternalBlue exploit. It doesn't drop any files on the disk but instead enables the installation of the DoublePulsar backdoor that lives in the kernel's memory. **How do non-malware attacks work?** Since non-malware attacks use default Windows tools, they manage to hide their malicious activity behind the legitimate Windows processes. As a result, they become nearly undetectable for most anti-malware products. **Main non-malware attack targets** The hackers need to obtain as many resources as possible while keeping their malicious activity

	undetected. This is why the majority of fileless attacks focuses on one of the two targets: • Windows Management Instrumentation (WMI) • PowerShell Depending on their targets, fileless attacks may either run in RAM or exploit vulnerabilities in software scripts. The attackers chose WMI and PowerShell for several reasons. First, both these tools are built into every modern version of Windows OS, making it easier for the hackers to spread their malicious code. Secondly, turning off any of these tools is not a good idea, since it'll significantly limit what network administrators can do. Some experts, however, suggest disabling WMI and PowerShell anyway as a preventive measure against fileless attacks. **4 common types of non-malware attacks** There are many types and variations of fileless malware. Below, we listed the four most common ones: **Fileless persistence methods —** the malicious code continues to run even after the system reboot. For instance, malicious scripts may be stored in the Windows Registry and re-start the infection after a reboot. **Memory-only threats —** the attack executes its payload in the memory by exploiting vulnerabilities in Windows services. After a reboot, the infection disappears. **Dual-use tools —** the existing Windows system tools are used for malicious purposes. **Non-Portable Executable (PE) file attacks —** a type of dual-use tool attack that uses legitimate Windows tools and applications as well as such scripts as PowerShell, CScript or WScript. **Non-malware attack techniques** In order to perform a non-malware attack, hackers use different techniques. Here are the four most frequently used ones: **WMI persistence —** WMI repository is used for storing malicious scripts that can be periodically invoked via WMI bindings. **Script-based techniques —** hackers may use script files for embedding encoded shellcodes or binaries without creating any files on the disk. These scripts can be decrypted on the fly and executed via .NET objects. **Memory exploits —**fileless malware may be run remotely using memory exploits on a victim's machine. **Reflective DLL injection —** malicious DLLs are loaded into a process's memory manually, without the need to save these DLLs on the disk. The malicious DLL can be either embedded in infected macros or scripts, or hosted on a remote machine and delivered through a staged network channel.
Return to Top	

HEADLINE	**04/26 Malware of mass destruction next WMD?**
SOURCE	**https://www.welivesecurity.com/2018/04/26/malware-mass-disruption-rsa2018/**
GIST	One might wonder why one of the final mainstage presentations at RSA 2018 had "Weapons of Mass Destruction" (WMDs) in its title? When ESET Global Security Evangelist Tony Anscombe finished with his presentation, however, no one was asking that question; instead what emerged was a better understanding of how the evolution of malware has led us to the digital weaponry of today and tomorrow. The central question of Anscombe's presentation was: Can malware be used as a weapon of mass destruction? He contends that it can and notes that we are at a tipping point where malware evolution has led us to the latest development in cyberweapons; this is what Anscombe coins "Malware of Mass Disruption." He defines this as the following:

- Any malware that targets infrastructure and thus could damage or disable services and could potentially cause death or serious bodily injury
- Any malware designed to inhibit first responders or emergency response from providing lifesaving treatment
- Any malware that targets health care or medical devices and could potentially cause death or serious bodily injury
- Any software that is intended to damage or disable medical systems or devices

Malware of Mass Disruption

Over the years, we have had some close calls that give a glimpse into the effect digital weapons can have. In 2017, the United Kingdom's National Health Service (NHS) was a major victim of the WannaCryptor (aka WannaCry, WCrypt) attack [ESET detects this as Win32/Filecoder.WannaCryptor.C, or less formally as "WannaCryptor.C" — Ed.].

According to a government report, at least 6,912 NHS appointments were canceled, with estimates that the total may be as high as 19,000. These numbers only reflect NHS hospital appointments – the impact on local physician visits is unknown. Within this number are 139 urgent referrals of patients who potentially have cancer.

It would not be unreasonable to consider a malware attack a 'weapon' when it does in fact affect the urgent health care of patients. If the WMD definition and title were adjusted to become Malware of Mass Disruption, then the WannaCryptor attacks would certainly be categorized this way.

Perhaps one of the most notorious attacks to cause disruption to society on a large scale was the 2015 malware known as BlackEnergy, which caused power outages in Ukraine, impacting 225,000 customers for up to six hours. The malicious actors responsible attacked three regional electric power distribution companies with synchronized and coordinated attacks within 30 minutes of each other and impacted multiple central and regional facilities.

And that was only the beginning. In 2016, a new attack, later attributed to malware dubbed Industroyer, deprived the capital city of Ukraine, Kiev, of power for approximately one hour. This attack differed significantly from BlackEnergy as it targeted Industrial Control Systems (ICS). By exploiting weaknesses in the software of the ICS devices, the attackers were able to control electricity substation switches and circuit breakers directly, ultimately controlling the delivery of power.

The critical infrastructure of a city might just be the crown jewel to a nation-state actor. Attacking the power infrastructure of a city, country or even a building has the potential to cause huge disruption, and, depending on the circumstances, endanger life. Imagine if an intensive care unit of a hospital lost power; the outcome could be fatal. While this is a hypothetical scenario, it may not be far from reality – if a cybercriminal can switch off the power to a city, they probably have the ability to switch off the supply to a building and, with the right resources, change the way any backup systems may operate.

"Using the word 'weapon' in association with malware may be a step too far for some people," noted Anscombe. But he points out an important malware history lesson, bringing attention to the first major attack against infrastructure, dubbed Stuxnet. "This showed, really for the first time, that a nation state could actually attack the infrastructure of another nation state by using malware as the tool or weapon," he said.

Since prominent infrastructure attacks like Stuxnet, various examples point to a conclusion that malware has the potential to "be a weapon in the arsenal of any government or organization that wants to inflict damage or disruption on another person, organization or country – or the world as a whole," he pointed out.

From notorious attacks like WannaCryptor, to aggressive blackouts caused by BlackEnergy and Industroyer, to attacks that potentially affect election outcomes, the reality exists that the bad actors

	creating and utilizing malware are disrupting our sense of safety, security and democracy. "I will leave you to decide whether to call these weapons," he concluded.
Return to Top	

HEADLINE	**04/26 Report: China seizes 600 bitcoin miners**
SOURCE	**https://www.theregister.co.uk/2018/04/26/china_600_computers_seized/**
GIST	Chinese media is reporting the seizure of 600 Bitcoin miners in the northern municipality of Tianjin, on the grounds of electricity theft. Coin mining is a popular activity in China, but like so many places, those operating big mining rigs find the rivers of gold dammed by high electricity prices. The Digiconomist Bitcoin Energy Consumption Index currently tags Bitcoin's total draw at nearly 63 Terawatt-hours, and reckons each transaction as costing 908 kWh. What better way to cut costs than to bypass billing entirely? That's what Xinhua and other agencies say happened in Tianjin: six people have been arrested because they allegedly bypassed the power meter in a junction box to get free power for their miners. The Xinhua report said the electricity company noticed a 28 per cent increase in line loss (implying an increased load current) on a circuit, and notified authorities. The report claimed the power thieves were trying to evade monthly bills of "hundreds of thousands of yuan" per month (100,000 yuan is currently around US$15,800). Meanwhile, prosecutors in Wuhan City's Hanyang District Procuratorate are about to commence a prosecution against two miners who used the same trick to steal electricity, before their arrest in 2017. China's prosecutor says the two, identified as Chen and Li, set up their rig in a house slated for demolition in March 2017, and used 49,100 yuan worth of power before they were cuffed
Return to Top	

HEADLINE	**04/26 Insider breach costs over $8.7M**
SOURCE	**https://www.infosecurity-magazine.com/news/insider-breach-costs-rise-to-87m/**
GIST	The cost of an insider-related breach has escalated to over $8.7m, according to the latest research from the Ponemon Institute. The analyst was commissioned by ObserveIT to poll 700 IT and security practitioners around the world in order to compile the 2018 Cost of Insider Threats study. While the cost of an insider security incident stood at nearly $8.8m, the average global cost of a regular breach according to IBM is $3.6m, less than half. The average insider threat also takes on average more than two months to contain, according to the report. Most respondents (64%) said negligent employees accounted for the majority of incidents, followed by malicious insiders (23%). All types of insider threat activity are increasing. Since 2016, the average number of incidents involving malicious insiders has soared by 53%, while employee/contractor negligence has increased by 26%. The average number of credential theft incidents has more than doubled over the past two years, increasing by 170%.

	That's fuelling an increase in imposter attacks – the most expensive type of insider incident at an average of $648,846. This is followed by malicious insider incidents ($607,745) and contractor negligence ($283,281). "Insider threats continue to threaten organizations across the globe, ultimately resulting in loss of mission critical data, downtime and lost productivity, and even reputational damage," said ObserveIT CEO, Mike McKee. "Understanding the growing costs and time associated with preventing and managing insider threats, organizations need to invest in a holistic cybersecurity solution to assist with real-time detection, deterrence, education and prevention." The latest Verizon DBIR found that insiders were to blame for a quarter (28%) of all breaches analyzed and that user error was a factor in 17% of breaches. A separate report from Gemalto released recently also highlighted the dangers of negligent insiders. Although accidental loss was the cause of just 18% of data breaches, it accounted for 76% of the total 2.6bn records compromised over the previous year, the security vendor claimed.
Return to Top	

HEADLINE	**04/25 Majority online banking systems w/flaws**
SOURCE	**https://www.scmagazineuk.com/two-thirds-of-online-banking-systems-in-2017-contained-high-risk-vulnerabilities/article/760956/**
GIST	Over the years, governments and cyber security experts have repeatedly urged businesses and critical industries to strengthen their cyber-defences to keep up with emerging threats and to ensure the security of enterprise and customer data. While cyber-criminals have spared no industry in their quest for financial gain or to destabilise economies, online banking systems were, and still are, prime targets for such entities as any security flaw can be exploited to impact hundreds of thousands of people and to gain access to millions, if not billions, of pounds. In 2015, a time when banks were swiftly adopting new digital technologies, introducing online banking services and shutting down brick-and-mortar branches with a vengeance, little heed was paid to how weak those newly-introduced online systems were vis-a-vis the capabilities of motivated cyber-criminals. According to Positive Technologies, 90 percent of online banking systems were found to contain high-risk critical vulnerabilities in 2015. This number had, in fact, increased remarkably from 78 percent of such systems in 2013-14, implying that the adoption of digital tools also made banks more vulnerable to threats such as SQL injections, unauthorised access to arbitrary user operations, and rounding attacks. At the same time, online banking apps, which customers were asked to download to seamlessly access banking services and products, were equally vulnerable to online threats. In 2015, 75 percent of banking apps on Android contained high-risk vulnerabilities compared to 33 percent of iOS apps. Positive Technologies' report indicates that UK banks have taken measures to plug security holes in their online banking systems and apps and as a result, such systems are not as vulnerable to external threats as they were a couple of years ago. For instance, compared to 90 percent in 2015, 56 percent of banking systems were found to contain high-risk vulnerabilities in 2017 and on an average, each web application contained 1.3 high-severity vulnerabilities compared to 4.2 in 2015. Despite such improvements, each e-banking system analysed in 2017 contained, on average, seven vulnerabilities, up from six in 2016, implying that banks focussed more

	in plugging the critical ones before shifting their focus to medium or low-risk flaws. The report revealed that not a single banking system could demonstrate the absence of low-risk, medium-risk or high-risk vulnerabilities, that almost half (45 percent) of such systems contained medium-risk vulnerabilities and only a third of online banking systems were free of critical vulnerabilities in 2017. A break-up of vulnerabilities impacting the security of online banking systems revealed that 75 percent of these systems contained cross-site scripting flaws, 69 percent had insufficient protection from data interception, 63 percent had insufficient authorisation (high-risk), 50 percent were vulnerable to sensitive data disclosure, and 31 percent were vulnerable to software version disclosure. Other vulnerabilities included insufficient protection from brute-force attacks and insufficient process validation. Considering only high-severity vulnerabilities in 2017, 63 percent of banking systems suffered from insufficient authorisation compared to 57 percent in 2016, 25 percent had two-factor authentication flaws compared to 71 percent in 2016, 19 percent had insufficient process validation compared to 14 percent in 2016, and 13 percent were vulnerable to arbitrary code execution compared to 14 percent in 2016. A look at the security of web applications run by UK banks revealed a worrisome picture. 94 percent of them were vulnerable to unauthorised access to client personal information and confidential banking data, 75 percent were vulnerable to access to sensitive information and configuration data, 50 percent were vulnerable to fraudulent transactions and theft of funds, and 31 percent were vulnerable to DDoS attacks on user accounts. The overall security of mobile banking apps wasn't much different to that of online systems, with 29 percent of all vulnerabilities being critical ones, 56 percent medium-risk and the rest of them being low-risk ones. In all, almost half (48 percent) of mobile banking apps had at least one critical vulnerability.
Return to Top	

HEADLINE	**04/25 Thailand seizes 'Hidden Cobra' servers**
SOURCE	**https://www.bankinfosecurity.com/thailand-seizes-hidden-cobra-command-and-control-servers-a-10903**
GIST	The Thai government says it has seized servers used by a group that's been tied to cyber espionage attacks, while preserving the servers for review by law enforcement agencies. Thailand's Computer Emergency Response Team, ThaiCERT, announced the takedown on Wednesday, saying it's working with law enforcement authorities as well as information security firm McAfee as part of an investigation into what the security firm has dubbed Operation GhostSecret. McAfee says the operation, which remains active, gives attackers advanced tools for conducting network reconnaissance, stealing information as well as deleting data. "The campaign is extremely complicated, leveraging a number of implants to steal information from infected systems and is intricately designed to evade detection and deceive forensic investigators," Raj Samani, McAfee's chief scientist, says in a blog post. "The implants vary considerably and although they share some functionality and code, they are categorized as different families." Malware families that have been used by the group of attackers include a new type of attack code called Proxysvc. Researchers have also found variants of Destover, which was used in the Sony Pictures Entertainment attack in 2014, as well as Bankshot, which was recently used to target the Turkish financial sector as well as financial services firms in other countries. McAfee says with "high confidence" that based on all the available clues, the APT group known as Hidden Cobra is behind the GhostSecret campaign.

	Attackers also expanded from targeting the financial sector to infecting organizations in additional sectors, including critical infrastructure, enterprise and healthcare.
Return to Top	

HEADLINE	**04/26 Report: tech supply chain vulnerable**
SOURCE	**http://www.homelandsecuritynewswire.com/dr20180426-federal-it-communications-technology-supply-chain-vulnerable-to-chinese-sabotage-espionage**
GIST	The U.S.-China Economic and Security Review Commission released a report entitled Supply Chain Vulnerabilities from China in U.S. Federal Information and Communications Technology, prepared for the Commission by Interos Solutions, Inc. The report examines vulnerabilities in the U.S. government information and communications technology (ICT) supply chains posed by China, and makes recommendations for supply chain risk management. The report issues a warning about the extent to which China has penetrated the technology supply chain, and calls on the U.S. government and industry to develop a comprehensive strategy for securing their technology and products from foreign sabotage and espionage. "China did not emerge as a key node on the global ICT supply chain by chance," the report says. "The Chinese government considers the ICT sector a 'strategic sector' in which it has invested significant state capital and influence on behalf of state-owned ICT enterprises." At the same time, Bejiing has moved to prevent other countries from using similar strategies to crack the Chinese market, accelerating indigenous production of IT and communications parts and requiring outside businesses to turn over their source code store data on Chinese servers and allow the government to conduct security audits on their products before gaining access to the Chinese market. Furthermore, the report argues that the U.S. government lacks an overall strategy to anticipate future developments in supply chain, identify potential threats and mitigate threats. The overall push for IT modernization means the government will increasingly rely on a web of complex supply chain operations that eventually originate with commercial suppliers in China. Laws like the Federal IT Acquisition Management Act and the Modernizing Government Technology Act put pressure on agencies to modernize through commercial-off-the-shelf products that are more likely to originate from China. Key findings: • Effective supply chain risk management is the ability to anticipate future developments in supply chains, identity potential threats to supply chains, develop threat profiles, and mitigate or address future threats to the supply chain. Federal government laws and policies do not currently address supply chain risk management comprehensively. • Chinese government's policies prioritize domestic production, extract intellectual property and technology from multinational companies in exchange for market access, use Chinese companies to further state goals, and target U.S. federal networks and the networks of federal contractors. These policies have heightened risks to the U.S. ICT supply chain, and to U.S. national and economic security. • Cyberattacks on supply chains will become easier—and more prevalent—as developing technologies such as fifth generation (5G) mobile network technology and the Internet of Things (IoT) exponentially increase avenues for attack. • ICT products have increasingly complex, globalized, and dynamic supply chains, many of which include commercial suppliers that source from China at multiple points within a single supply chain. For example, an average of 51 percent of shipments to seven leading federal ICT providers originate in China (see Exhibit 1).

	• It is unlikely that political or economic shifts will push global ICT manufacturers to dramatically reduce their operations in China or their partnerships with Chinese firms. A national strategy is needed for supply chain risk management of U.S. ICT, and it must include supporting policies so that U.S. security posture is forward-leaning, rather than reactive and based on incident response. • To minimize risks, the federal government should: centralize the leadership of federal ICT supply chain risk management efforts, link federal funding to supply chain risk management, promote supply chain transparency, and craft forward-looking policies.
Return to Top	

HEADLINE	**04/27 Bitcoin frenzy settles down**
SOURCE	**https://www.reuters.com/article/us-crypto-currencies/bitcoin-frenzy-settles-down-as-big-players-muscle-into-market-idUSKBN1HY0W7**
GIST	LONDON/NEW YORK/SINGAPORE (Reuters) - After bouncing up, falling down and keeping investors on the edges of their seats, bitcoin may be maturing into a period of relatively boring stability, experts say. A worldwide wave of regulation has led to a collapse in trading volumes. Cryptocurrency advertisements are disappearing from top internet pages, and bitcoin no longer dominates Google searches. As investors try to figure out what bitcoin wants to be when it grows up, the best-known cryptocurrency is going through somewhat of an existential crisis. “It needs a new narrative,” said Nicholas Colas, New York-based founder of investment research firm DataTrek. “There is every chance that if there is some sort of institutional involvement, there could be a move higher.” Bitcoin rallied 25 percent in April after crashing 70 percent from a high near $20,000 late last year. The cryptocurrency landscape has indeed changed. Mom-and-pop investors who drove bitcoin’s skyrocket rise in 2017 have been pushed aside by government bans on trading, and replaced by cryptocurrency funds, wealthy individuals and established financial firms. The bigger players can make bigger moves, but their trades are often obscured by screens on over-the-counter (OTC) brokerages and matching platforms. They are also less likely to chase sudden swings in bitcoin’s value, being more interested in the potential of unproven but promising blockchain technology. Average daily traded volumes across cryptocurrency exchanges fell to $9.1 billion in March and to $7.4 billion in the first half of April, compared with almost $17 billion in December, according to data compiled by crypto analysis website CryptoCompare. Several exchanges saw their daily trading volumes drop by more than half between December and March, including Bitfinex, Poloniex, Coinbase and Bitstamp, the data shows. Cryptocurrencies’ biggest-ever trading day was Dec. 22, when volumes topped $30 billion, according to CryptoCompare. On April 8, volume sagged to $4.6 billion, the weakest day since last October, according to the data. The theory that bigger institutions will make bitcoin markets less volatile and more liquid has grown as new OTC exchanges spring up, carrying names such as Circle, Octagon Strategy, Cumberland and Kraken.

	Digital exchange Gemini's new block trading product allows high-volume trades that will be invisible to other traders until the orders are filled. Cumberland, one of the biggest block traders, has counterparties in more than 35 countries and quotes two-way prices in about 35 crypto assets. Gatecoin, a Hong Kong-based crypto exchange, saw retail volumes plunge from peaks of $100 million a day last September, said Aurelien Menant, its founder and chief executive. But, he said, as institutional players enter the market, OTC trades hidden from view have pushed up overall volumes in a way that doesn't show up in data. Gatecoin also operates an OTC platform. Few institutions have gone public about their plans to trade cryptocurrencies, and many asset managers say they still aren't sure the digital currency is more than a fad. But a Thomson Reuters survey this week found one in five financial institutions is considering trading cryptocurrencies in the next 12 months. Of those, 70 percent said they planned to start trading in the next three to six months. In the meantime, the price of bitcoin may be stabilizing, at least on paper. The futures market BTCc1 shows bitcoin staying nearly flat - between $8,900 and $9,050 - until September.
Return to Top	

Terror Conditions

Top of page

HEADLINE	**04/26 Italy detains asylum seeker in terror plot**
SOURCE	**http://abcnews.go.com/International/asylum-seeker-instructed-drive-vehicle-crowd-italians/story?id=54746665**
GIST	Italian security forces have detained an asylum seeker from Gambia and accused him of planning a terror attack with a vehicle. Alagie Touray, 21, was arrested outside the Licola mosque in southern Italy last Friday. He is a member of ISIS, Italian authorities said. Touray was picked up at the request of the Naples public prosecutor after a joint investigation by the Carabinieri and State Police who had received a tip from Spanish intelligence. Touray's arrest was announced today at a news conference in Naples. During questioning, authorities said, the Gambian admitted to having received a request via the messaging app Telegram where he was told to "crash a vehicle into a crowd," Naples prosecutor Giovanni Melillo, said at the news conference. Touray admitted having received instructions to commit a terror attack but, according to Prosecutor Melillo, the Gambian said he had no intention of carrying out the attack. The examination of his Telegram uncovered other alarming messages, including those where he asked people "to pray for him" and that "he was on a mission," authorities said. Touray also recorded a pledge of allegiance to the leader of the Islamic State (ISIS), police said, provided a transcript and image from the message where Touray said, "I swear allegiance to the Caliph of Muslims Abu Bakr Al Quaraishi Al Baghdadi, and to listen to him and obey him in difficult and easy times, on this 2nd day of Rajab and Allah is witness to what I say," The Gambian arrived in Sicily by boat with 800 other migrants in March 2017 before requesting political

	asylum, which was still under review, authorities said.
Return to Top	

HEADLINE	**04/27 Confronting terrorism online**
SOURCE	**https://lawfareblog.com/whose-responsibility-it-confront-terrorism-online**
GIST	This week, Facebook and YouTube announced new data on removal of terrorist content on their platforms. Facebook also released its internal document clarifying what content stays online and what is deleted. YouTube, under Google's broader efforts, also stated that it is getting "faster" at takedowns with an increased number of human reviewers vetting questionable content. Some of those in counterterrorism policy circles and Capitol Hill are fervent advocates of technology behemoths stepping up enforcement of their terms of service and will likely praise these new releases. Ultimately, however, the responses detailed by Facebook and YouTube are another iteration of a decade-long strategy, as the government continues to delegate online counter-terrorism responsibilities to private industry. As a former congressional staffer, a member of the intelligence policy community, and now an academic researcher, my career has traced the growth of terrorist use of the internet. During my time as a staffer, I wrote letters on behalf of the chairman of the Senate Committee on Homeland Security and Governmental Affairs calling for technology companies to remove terrorist videos from their servers, and I examined how terrorist groups like al-Qaeda and al-Shabaab have adeptly used social media to radicalize and recruit Americans to their cause. As a researcher, I've studied the online environment as well—but I've become concerned that this singular focus on the internet ignores the importance of peer-to-peer terrorist recruitment. Over the past decade, foreign terrorists command and capability in the digital sphere has drastically evolved. But our responses to this have not adapted with the same efficiency. The government's ability to adapt to this changing environment is sharply limited by its outsourcing of the responsibility to prevent and confront terrorists' use of the internet to private companies. To figure out how best to respond to evolving threats, it is useful to reflect on how the relationship between governments and private tech companies evolved and how this process of delegation came to be. Historical Overview In 2007, a bipartisan group of senators and members of the House became increasingly concerned with terrorist use of online platforms. At the time, the most striking example was a series of YouTube videos depicting the so-called "Baghdad Sniper." These videos, usually set to music and spliced into quick clips, showed an Iraqi insurgent attacking U.S. soldiers in Iraq. The videos raised questions for congressional staffers—chiefly, "Is an American company comfortable with grotesque videos of U.S. military officers being killed on its platform?" The answer, after an influx of public letters, was a resounding "no." As a result, YouTube announced updates to its community standards to address videos with violent imagery. Shortly thereafter, YouTube also implemented a "terrorist flag" feature which allowed users to identify extremist content for review and ultimately removal. This was one of the first instances in which private companies took initiative to police their own sites after being subject to public pressure. At the same time, debates surrounding the efficacy of content removal continued within counterterrorism communities. One side posited that companies should remove terrorist propaganda from mainstream websites due to the material's perceived ability to radicalize its viewers. The other side argued that the risk of radicalization from accessing content was low and that allowing it to remain online would aid law enforcement and intelligence agencies. To a large extent, these arguments remain defining characteristics of contemporary debates within the government regarding the nexus of technology and terrorism. In the midst of this schism, one side of the debate tried to tip the scales in their favor. A surreal and entirely off-the-books meeting between a high-ranking intelligence official and a congressional colleague of mine occurred at a D.C. park. The colleague, who had been advocating for content removal, was facing

pressure from his executive branch counterparts on the operational side. While sitting on a park bench, the intelligence official made clear that parts of law enforcement and intelligence communities preferred such material to stay online. In their view, it acted as a useful honey trap to track terrorists—and taking down online content could endanger both operations and lives.

While the meeting may have caused a temporary pause, it ultimately did not guide Capitol Hill's view on confronting terrorist content online. As terrorism receded into the background noise of larger news stories and public pressure ebbed, efforts by both Congress and technology companies came almost to a standstill. Government approaches were essentially limited to awareness training, which focused on demonstrating to primarily Muslim-American communities around the country how groups like al-Qaeda use the internet to target young people, so that parents could protect their children. The awareness trainings, while important, were too sporadic to be the silver bullet.

With the rise of the Islamic State, the issue of terrorists' use of the internet quickly forced its way back onto the political agenda. For policymakers, advocating content removal is a relatively easy ask with little blowback; it allows them to look tough on terrorism while requiring little concrete follow-through on the government's part. In January 2016, high-ranking intelligence officials traveled to Silicon Valley to encourage the major technology companies to do more to police problematic content on their platforms. The White House later brought together advertising marketers from Madison Avenue, technology experts from Silicon Valley, and producers from Hollywood to tackle the question of how to respond to onslaught of Islamic State propaganda. Like many things developed within the cocoon of the National Security Council at that time, there was little interagency buy-in, and this initiative eventually failed to produce tangible results from a lack of sustained coordination.

In the U.S. and abroad, pressure on the technology companies mounted as the Islamic State remained a critical threat in the eyes of many Western countries and their constituents. Out of a mixture of a sense of responsibility and public pressure, likely combined with a desire to prevent hasty regulation by Capitol Hill, some technology companies responded with show of force. The companies colloquially known as the "Big Four"—Microsoft, YouTube, Twitter, and Facebook—announced the formation of the Global Internet Forum to Counter Terrorism. In partnership, these companies developed a "hashing" database to share information to flag and moderate extremist materials. YouTube and Facebook greatly increased the number of human reviewers for terrorist content, while Twitter, the platform of choice amongst jihadists in 2015, also took concerted steps to make its platform less hospitable to violent extremists. With the precedent set by Twitter's biannual transparency reports, major tech providers, including Facebook and YouTube, now provide regular updates on their progress and methods of combating violent extremism in regular press releases.

Going Forward

Responses driven by industry, largely at the behest of the U.S. government, have certainly demonstrated some significant successes. Major social media providers continue to remove terrorist content from their websites at a much faster rate than before. However, this approach may not be nimble enough to respond to current developments in how terrorists utilize the internet.

While the Islamic State still uses mainstream sites like Twitter to push its propaganda, it has largely shifted to niche platforms in response to content removal. Many of these platforms, such as justpaste.it, lack the personnel and budget to remove extremist content. Some have no interest whatsoever in addressing terrorist use of their platforms: As many of these companies are based outside of the United States, the Damocles sword of possible regulation does not hang over their head.

Public pressure also has less power when free expression at all costs is embedded in the culture of these companies. Currently, the most active platform for distributing Islamic State propaganda is the messaging application is Telegram, whose CEO, Pavel Durov, has been ardent in his company's founding principles: "I think that privacy, ultimately, and our right for privacy is more important than our fear of bad things happening, like terrorism." As demonstrated by the Russian government's recent, botched attempt to ban the use of Telegram, Telegram's resistance to calls for censorship only builds their reputation among their

	users. There are persistent questions that come with allowing industry to set their own standards. For years, Americans have faced the question of whether they are comfortable with the standards that large technology companies and social media providers use for content removal. But with the online terrorism environment rapidly changing, the question is now whether those standards can transfer to newer and smaller companies, or companies with different political interests and outlooks. What's more, newer companies will likely not have the same level of sophistication in understanding the threat as do larger companies such as Facebook, which employ hundreds of counterterrorism analysts. How will these companies handle content that walks the fine line between advocating violence and providing the mood-music of extremism? At the moment, a Salafist imam from Michigan, Musa Jibril, is the second-most-cited radical preacher by Islamic State followers online. He trails only Anwar al-Awlaki in his prominence—but Jibril's online sermons never cross the line of calling for overt violence. Should his material stay online? Should that assessment change if he is discovered to have influenced, even if indirectly, attacks in the West—and if it does, will that mean that are our content standards are being set by of the news of the day? These are critically important questions to answer if the U.S. government continues to address the future online dynamics of terrorism through ad-hoc delegation of counterterrorism responsibilities to tech giants. As a result of this approach, companies like Twitter, Facebook, and Google have ample leeway to determine their standards for content removal. But the U.S. government should not assume that other social media providers with different interests will earnestly adopt these standards, especially if they lack the wherewithal or interest to do so. As terrorist groups adapt to the changing landscape of the online space, it is worth asking whether U.S. government policies that depend on overwhelming initiative from the tech sector will be able to adequately respond—and whether the government's ceding responsibility to the private sector is the right way forward.
Return to Top	

HEADLINE	**04/27 ISIS propaganda websites targeted**
SOURCE	**https://www.huffingtonpost.co.uk/entry/islamic-state-europol-amaq-shutdown_uk_5ae2e84ee4b04aa23f21f616**
GIST	Some of the Islamic State's most prominent propaganda websites have been hit by a coordinated cyber strike by European countries, in an attempt to curb the terror group's online influence. The "simultaneous multinational takedown" of Isis-branded media outlets on Wednesday and Thursday targeted the Amaq News Agency, al-Bayan radio, Halumu and Nashir news. Rob Wainwright, executive director of Europol, the EU's law enforcement agency, said the "groundbreaking" operation had involved the UK, US and France along with five other countries. "We have punched a big hole in the capability of Isis to spread propaganda online and radicalise young people in Europe," he said. The attack aimed to disrupt the technical resilience of the terrorist online infrastructure, Wainwright added. The seized data is expected to help authorities identify the administrators behind Isis media outlets and "potentially radicalised individuals on European soil and beyond". Since 2015, Europol said the site had launched its own software and developed "highly resilient online infrastructure hosting". As of December 2017, the entire range of Isis propaganda was available in at least nine different languages, as well as on a wide range of online services, such as mailed newsletters and add-on extensions for the most common browsers, Europol said.

	The crackdown began in 2015 after Europol informed all EU Member States about the rise of the Amaq News Agency and its capabilities. In August 2016, EU Member States and non-EU countries took down Amaq's mobile application and web infrastructure, but this led the "propagandists to build a more complex and secure infrastructure to prevent further disruption from law enforcement". In June 2017, a second strike, targeted part of the news agency's web assets and infrastructure. Serves seized during that operation, Europol said, led to the identification of radicalised individuals in more than 100 countries worldwide. Europol Commissioner Dimitris Avramopoulos said the latest operation showed "our global strength and our unwavering resolve to fight against terrorist content online". He added that IS was now "no longer just losing territory on the ground – but also online. We will not stop until their propaganda is entirely eradicated from the Internet."
Return to Top	

HEADLINE	**04/26 World Cup 2018 terror warning**
SOURCE	**https://www.express.co.uk/news/uk/951657/world-cup-2018-terror-warning-isis-volgograd-england-opener**
GIST	With almost thousands of England fans descending on Volgograd for the game, the attacks are likely to be mounted against fans using vans and knives or bombs blasts on buses and trains, with Moscow and St Petersburg also at risk. ISIS would be targeting Volgograd because of its proximity to the North Caucasus region, which was the largest source for foreign fighters in Syria and Iraq counting almost 3,500 soldiers. More than 400 hardliners are now back in the soviet region and security experts believe ISIS is planning a terrorist attack at the opening game to revenge the airstrikes in Syria launched by President Vladimir Putin. Chris Hawkins, a senior analyst at Jane's Terrorism and Insurgency Centre, said: "There are numerous terrorism threats affecting the World Cup. "The main one, as with the rest of Russia, comes from lone actors with low capabilities. Tactics will likely include knives and vehicle attacks targeting fans visiting games or the surrounding areas. "Aspirational targets will include match days, particularly in Moscow and St Petersburg – the two cities that will have the largest concentration of foreign visitors, with Moscow hosting the key fixtures of the World Cup, including the final and the opening fixture. "Sochi and Volgograd are two other cities at heightened risk due to their proximity to the North Caucasus region meaning they are logistically viable cities for militants to stage attacks." The terror expert added that returning ISIS fighters pose as a serious threat due to weapons and bomb-making experience: "These fighters have had combat experience and have had training in operating military-grade firearms as well as manufacturing IEDS." England World Cup opening match against Tunisia is on June 18 at Volgograd Arena, but many fans are expected to stay in St Petersburg or Moscow.
Return to Top	

HEADLINE	**04/26 Arrested woman had USB w/police info**
SOURCE	**https://www.buzzfeed.com/mitchprothero/french-police-fear-isis-militants-have-their-names-and?utm_term=.tp4R0A2Ow#.myoAzqOMB**
GIST	French police investigating a woman for suspected ties to ISIS have made a chilling discovery, according to French police officials and prosecutors: The arrested woman had a USB drive that contained the personal details of thousands of French police officials. That's raised fears that a similar data breach may have helped an ISIS militant carry out the notorious June 2016 murder of a French police commander and his domestic partner, a civilian police employee. The USB was discovered last October during raids on apartments and properties linked to the 25-year-old woman, who's been identified publicly only as Mina B. She now stands accused of being in direct contact with an ISIS-directed group in the Belgian city of Verviers that was raided in January 2015. Two extremists were killed in that raid. Phone intercepts linked Mina B. to the Verviers group, and police launched an investigation that culminated April 9 with charges that Mina B. had helped a friend leave France to join ISIS in Syria and Iraq. At that time, police also announced that they had discovered the USB drive in her apartment. The USB drive, according to French investigators, had been partially erased. Reconstruction of some of the drive's contents, however, recovered at least one personnel database, from 2008, that included a raft of details about police officers, including home addresses and vehicle information. Specialists are still trying to reconstruct the USB's full contents. "This is a disaster," said one French police officer who works undercover on counterterrorism operations and cannot be identified. The officer pointed out that while the restored database dates to 2008, "that's only 10 years and many of the officers are still in service." He added, "The information contains all the information one needs to stalk and murder hundreds of police officers in their homes, which as you know has already happened." The officer was referring to the June 13, 2016, double murder of Jean-Baptiste Salvaing, a police commander in the Paris suburb of Les Mureaux, and his girlfriend, Jessica Schneider, 36, who was an administrative assistant in the police station at Mantes-la-Jolie, another Paris suburb. The accused killer was Larossi Abballa, who stabbed Salvaing several times outside the victims' home, before slitting Schneider's throat inside the home. He then streamed a statement supporting ISIS before French police shot him dead. Details for Salvaing and Schneider were not part of the recovered data, according to prosecutors, but Mina B. has been indicted with six others in the Salvaing case as investigators try to determine if Abballa received any assistance or information from her. Investigators also have determined that a major in the French police, Maryline Bereaud, was at least partially responsible for the data breach. They say that Mina B. was friends with Bereaud's daughter and that Mina B. had been a guest in Bereaud's home for several months in 2016. Bereaud, who was the chief of police in Yvelines, another Paris suburb, has been arrested and charged in relation to the leak. French news reports have quoted a police union official anonymously as saying that Bereaud had allowed Mina B. to stay in her home as a favor to her daughter. "It was a young girl who had been thrown out by her family, she sheltered her for a while at the request of her daughter. But she never saw signs of radicalization at home," said the union spokesperson.

	Investigators have determined that Bereaud and her daughter had no previous contact with Abballa but that Mina B. was part of his radicalized circle. "The coincidence that the suspect with the USB drive knew Abballa is a difficult one for police to accept," said the French police officer. "To have a list of police officers' home addresses and be in contact with a terrorist who murdered two police at their home, and we haven't been able to determine how he found their address? It's a big thing to tell me this isn't related." French police and internal security services face massive security concerns from terrorism with thousands of potential militants flagged for surveillance as part of the nation's "S List," which collects internal threats to the French state.
Return to Top	

HEADLINE	**04/26 US stepping up operations against ISIS**
SOURCE	**https://www.washingtontimes.com/news/2018/apr/26/james-mattis-sees-re-energized-syria-mission-again/**
GIST	The U.S. is stepping up military operations against Islamic State remnants in Syria, along with other extremist organizations fighting to fill the vacuum in the wake of Islamic State's defeat in the country, Pentagon chief James Mattis told Congress Thursday. The escalation, outlined in testimony to the Senate Armed Services Committee Thursday, comes after a raging internal debate in the U.S. government after President Trump expressed a desire to withdraw U.S. forces from Syria with the Islamic State terror group in his words nearly defeated. But Mr. Mattis and U.S. military commanders pushed back, warning a U.S. withdrawal could allow Islamic State to regroup, while leaving the Syrian government and its Russian and Iranian allies a free hand to re-establish control of the country. "Right now … we are not withdrawing" from Syria, Mr. Mattis told lawmakers. " … You will see a re-energized effort against the Middle Euphrates River Valley in the days ahead" against Islamic State, as well as other remaining pockets of territory still held by the terror group. France has agreed to send a contingent of special forces to reinforce the mission against Islamic State in Iraq, said Mr. Mattis. The deployment comes on the heels of French President Emmanuel Macron's first official visit to Washington earlier this week. Asked if local allies working with U.S. forces against Islamic State could handle the mission, "I am confident that we would probably regret it."
Return to Top	

HEADLINE	**04/26 Study: more 9/11 cancer burden cases**
SOURCE	**https://www.washingtontimes.com/news/2018/apr/26/cancer-burden-among-911-firefighters-and-first-res/**
GIST	More cancer cases than previously thought are expected among firefighters and rescue workers who responded in the aftermath of the Sept. 11, 2001, terrorist attacks on the World Trade Center, according to research published Thursday in the Journal of the American Medical Association. The latest study, conducted by the World Trade Center Health Program, accompanied research on improving early detection of multiple myeloma, a blood cancer and one of the top 15 certified cancers found among those exposed to the toxic atmosphere at ground zero in lower Manhattan. "In 2011 we, meaning our research team here, were the first to show that the cancer rates might be

	elevated in the WTC exposed population," FDNY World Trade Center Health Program researcher Dr. Rachel Zeig-Owens told The Washington Times. The WTCHP was established that year with the passage of the James Zadroga 9/11 Health and Compensation Act, named in honor of the New York City police officer who died of an aggressive respiratory disease that was later confirmed to have developed from breathing the air at ground zero in the aftermath of the terror attacks. The program provides complete medical coverage for first responders and survivors for conditions developed as a result of being exposed to toxic elements from the terror attacks in New York City, Pennsylvania and the Pentagon. Today, 69,612 responders and 14,308 survivors are registered with the program. As of December, there are 6,866 responders and 1,433 survivors who are diagnosed with cancer. At least 304 responders and 30 survivors have died from cancer, according to WTCHP statistics. The latest research by Dr. Zeig-Owens and colleagues estimates that new cancer diagnosis will increase at a higher rate than previously thought, with 2,960 new cancer cases between 2012 and 2031. Medical costs are expected be over $235 million for first-year treatment. Previous estimates had 246 less cases. "We project that the FDNY-WTCHP cohort will experience a greater cancer burden than would be expected from a demographically similar population," the authors wrote. "This underscores the importance of cancer prevention efforts and routine screening in WTC-exposed rescue and recovery workers." The three cancers expected to increase among this population include prostate, thyroid and melanoma cancers and few lung, colorectal and kidney cancers, the study read. "What it really does is show the continued need for cancer screening and that the risk may be elevated for years to come due to these exposures," Dr. Zeig-Owens said. "What also is helpful for the WTC health program is to know that it needs to plan and anticipate for the elevated costs of treatment as the years go on." The program is working on multiple studies examining various cancers, their risk and early detection. The latest, also published Thursday in JAMA, focuses on multiple myeloma, a cancer of the blood, specifically affecting plasma cells, integral to the functioning of the immune system. Dr. C. Ola Landgren, chief of the myeloma service at Memorial Sloan Kettering Cancer Center, said he and others were motivated to study this same population after years of seeing several newly diagnosed patients at younger ages and with more aggressive forms of the disease than normal. "That prompted us to reach out to the FDNY to make a collaborative study," Dr. Landgren told The Times, "to address these observations. That's really what prompted us from the clinical side to reach out."
Return to Top	

HEADLINE	**04/26 Challenge: tracking terror financing**
SOURCE	**https://www.wsj.com/articles/new-financial-transaction-methods-pose-challenge-in-terror-fight-officials-say-1524740047**
GIST	PARIS—President Emmanuel Macron called ministers from over 70 countries to Paris on Thursday in an effort to coordinate a crackdown on new terror-financing methods that French officials say pose a growing threat to global security.

Justice and finance ministers gathered at the Organization for Economic Cooperation and Development in Paris to look for ways to gather and share intelligence on how terrorist organizations like Islamic State and al Qaeda collect, move and store the finances that sustain them.

"It is the lifeblood of the war. It is essential to look at this very seriously and pre-empt the changes taking place," Paris prosecutor François Molins, who handles terror investigations in France, said on French radio Thursday.

Governments face an increasingly complex challenge tracking terror finance because of the changing technology of transactions. France will push delegates at the conference to look for ways to better identify users of prepaid cards and electronic wallets and strengthen regulation of crowdfunding websites that are increasingly used by terror groups.

There are also "high risks" associated with the transfers by mobile telephone because it is hard to identify recipients of funds, French officials said.

France says the large sums of money in circulation could spark a resurgence of terrorist organizations despite the military collapse of Islamic State in Syria and Iraq. Islamic State is estimated to have had revenues of around €1 billion a year between 2014 and 2017, and is now seeking ways to amass small international donations, French officials say.

"The successes in Syria and Iraq might make us think we are confronted with a declining threat, but the reality is very different," an advisor to Mr. Macron said.

"It feels like we are in a sprint because there is a sophistication of instruments," the advisor said.

The closed-door conference, dubbed "No Money for Terror," began Wednesday with talks between some 450 terror finance experts and intelligence officials, and will conclude later Thursday with a public speech from Mr. Macron.

Mr. Macron, who returned earlier from a three-day U.S. state visit, is pushing for a more multilateral approach. French officials hope delegates will sign up to a joint declaration that could be submitted to international organizations including the United Nations.

"I am optimistic that the discussions over the coming days will mobilize new efforts in the fight against terrorism," said U.S. Treasury Secretary Steven Mnuchin, who is attending the event.

International Monetary Fund chief Christine Lagarde and head of the World Bank President Jim Yong Kim are also attending.

Delegates will also examine how tracking transactions can be used to gather intelligence and anticipate possible attacks. Paris prosecutors working with financial investigators to track transactions in recent years have identified 416 donors on French soil and 320 recipients in Turkey and Libya, helping them identify jihadists who traveled to Iraq and Syria or those who are now looking to return to France.

Most middle eastern countries are represented at the conference, with the notable exception of Iran. Iran is on the blacklist of the Financial Action Task Force, an intergovernmental group of 37 that combats money laundering and terror financing. French organizers also refused to invite Iran amid tensions between Tehran and Arab states.

Return to Top

HEADLINE	**04/26 Afghan official: Taliban killed 7 soldiers**
SOURCE	**http://abcnews.go.com/International/wireStory/afghan-official-deputy-governor-killed-taliban-54744467?**

GIST	A Taliban attack on an Afghan army security post in the country's northern Kunduz province has killed at least seven soldiers, a defense spokesman said Thursday. Mohammad Radmanish, the deputy spokesman for the Ministry of Defense, said the attack took place on Wednesday night in the remote Dashti Archi district in Kunduz. A gunbattle lasted several hours and along with the seven killed, one soldier was wounded, Radmanish said. He added that 15 Taliban fighters were also killed and 13 were wounded. However, a local hospital chief, Rahimbakesh Danish Karimi, gave a higher casualty toll for the military, saying bodies of 13 soldiers and nine wounded in the attack were brought to his hospital in Thakhar province, which is the closest medical facility to the attack site. The conflicting casualty reports could not immediately be reconciled as is common in the aftermath of such attacks. No militant group has claimed responsibility for the attack but the officials blamed the Taliban.
Return to Top	

HEADLINE	**04/27 Military judge rules in landmark decision**
SOURCE	**http://www.foxnews.com/us/2018/04/27/us-already-fighting-al-qaeda-before-911-military-judge-rules-in-landmark-decision.html**
GIST	The U.S. was already at war with Al Qaeda before hijacked planes hit the Twin Towers and Pentagon and crashed in Pennsylvania, a U.S. military judge presiding at the pretrial of alleged 9/11 attack plotter Khalid Sheik Mohammed and others ruled this week. The landmark decision will pave the way for a trial of the accused 9/11 mastermind and four alleged abettors by military commissions at Guantanamo Bay, Cuba, the Miami Herald reported. Lawyers for the alleged conspirators tried to convince the military commission that since the U.S. entered the war against Al Qaeda only after the Sept. 11, 2001, attacks, the defendants can face trial only in federal, civilian courts -- not before military commissions. A lawyer for Mustafa al Hawsawi -- a Saudi man accused of supporting at least seven of the 19 hijackers -- argued that his client allegedly helped some of the hijackers with funds and travel to the U.S. before the American government was at war with Al Qaeda. Attorneys for another alleged conspirator, Ammar al Baluchi, claimed the war began when the U.S. invaded Afghanistan on Oct. 7, 2001. Prosecutors argued the war between the U.S. and the terror group began with Osama bin Laden's 1996 "Declaration of Jihad Against the Americans," according to the newspaper. The president signed an executive order giving his defense secretary 90 days to recommend whether those captured in the battlefield should be sent to Gitmo; Jennifer Griffin reports for 'Special Report.' But the judge, Army Col. James L. Pohl, wrote in a 20-page ruling that it's "unnecessary to decide a date certain for commencement of hostilities," asserting that the U.S. was at war with Al Qaeda prior to 9/11, as two presidents have said in the past. According to the ruling, President George W. Bush formed the military commissions to prosecute the culprits of the attacks, while President Barack Obama signed the Military Commissions Act of 2009 that "contemplates prosecution for offenses occurring 'on, before or after Sept. 11, 2001.'" "The overall armed conflict against al-Qaida — a transnational terrorist organization operating primarily

	outside the United States — might itself be viewed as an anomaly under pre-Sept. 11, 2001, law of war standards," Pohl wrote. "However, the law of war is not static, and its precise contours may shift to recognize the changing realities of warfare. Military commissions by their nature are intended to have sufficient flexibility to address the needs presented by the armed conflict they address."
Return to Top	

HEADLINE	**04/27 Turkey detains 4 senior ISIS militants**
SOURCE	**http://abcnews.go.com/International/wireStory/reports-turkey-detains-senior-islamic-state-militants-54773618?**
GIST	Turkey's state-run news agency says Turkish authorities have detained four suspected senior Islamic State extremists in an operation in the Aegean coastal city of Izmir. Anadolu Agency said Friday the suspects include the group's so-called "emir," or ruler, of Deir el-Zour, a major city in eastern Syria, and its environs. It described the other three suspects as senior operatives within the extremist group. Hurriyet newspaper said the four were captured as part of a joint operation by Turkey's intelligence agency and police anti-terrorism units. The suspects were hiding among a group of Syrian refugees planning to cross into Europe, the newspaper reported. The four are being questioned by anti-terrorism police in Izmir. Police in Izmir confirmed the operation but could not immediately provide details.
Return to Top	

Suspicious, Unusual

Top of page

HEADLINE	**04/26 New US 24-hr precipitation record set?**
SOURCE	**https://www.wunderground.com/cat6/new-us-24-hour-precipitation-record-4969-kauai-hi-april-15**
GIST	The National Weather Service in Hawaii reported on Wednesday that preliminary data from a rain gauge on the north shore of Kauai at Waipa, one mile west of Hanalei, received 49.69” of rainfall over the 24-hour period ending at 12:45 pm April 15. If verified, this would break the all-time U.S. 24-hour rainfall record of 43.00” in Alvin, Texas set on July 25 – 26, 1979, during Tropical Storm Claudette. The record-setting rains on Kauai were due to an upper-level low located to its west on April 14 - 15, combined with a surge of rich low-level moisture. This set-up brought radar-estimated rainfall rates of 2 – 4” per hour to the north shore of the island. The National Weather Service office in Honolulu noted that the rain gauge where this new data was downloaded from "is operated by the Waipa Foundation which is a non-profit organization. Data from the gauge are not telemetered for real-time display and are used for watershed modeling and monitoring studies." In the coming months, data from this gauge will be reviewed by the National Climatic Extremes Committee to determine whether this instrument is reliable enough to accept as a new U.S. record.
Return to Top	

HEADLINE	**04/27 Cars in Europe calling police accidentally**
SOURCE	**https://www.forbes.com/sites/davekeating/2018/04/27/cars-in-europe-are-accidentally-calling-the-**

	police/#60a763c74baf
GIST	It's been less than a month since European Union legislation took effect requiring all new cars to have the eCall system, which automatically calls emergency services in the event of an accident. But already, emergency operators are identifying teething problems. The eCall system automatically calls 112, the European equivalent of America's 911, after a collision. That number is automatically redirected to local emergency services across the EU. It's a complicated endeavour, particularly because it requires coordination and standardisation between the EU's 28 member states. This week emergency service professionals from across the continent gathered in Ljubljana, Slovenia for the annual conference of the European Emergency Number Association to discuss how the implementation is going so far. One consistent theme emerged: operators are getting too many false e-calls, which is proving a distraction from their work. Though the system has only been required for a month, it's been around for some time. It was first developed in 2001 as part of a German youth science competition. The EU chose it from several competing technologies to be the basis of the legislation, first put forward in 2013. Some European countries have rolled out eCall early. Slovenia introduced it in December 2015, and Italy deployed a pilot program in selected regions in May 2017. Sweden adopted eCall in October last year. Spain has also been an early adopter. Iratxe Gomez Susaeta, an emergency management expert who has been consulting with operators during the roll-out, said at the conference that false calls have been a problem so far. "There have been false eCalls during repairs or checkups, or people unintentionally pressing the SOS button – particularly children," she said. The system is meant to kick in only in the event of a serious accident, calling 112 and wirelessly deploying airbags and impact sensor information. It then uses Galileo, the EU's equivalent of America's GPS satellite system, to send information about the vehicle's location to emergency services. A microphone and speaker in the car enables to occupant to communicate with dispatchers. But the alert can be triggered while the car is being repaired or dismantled. If the mechanic doesn't hear the emergency service personnel trying to contact the car, first responders may be deployed to the location, wasting precious resources and time. Gomez Susaeta said so far these false calls and tests of the system have represented most of its use in some places. "We're off to a very slow start. Some haven't even received any real eCalls yet. It's been less than a month, and some have only received test calls or false eCalls. They're also getting lots of test calls in a live environment, which is creating a lot of confusion" Luca Bergonzi, a sales executive with the Beta 80 group in Italy, which is advising emergency services on the roll-out, agreed that false calls have been a problem so far. "End-of-life or vehicle inspection can trigger false eCalls, or automatic alarms used for security services," he said. "Companies are looking at a workaround. Public safety answering points should develop procedures to screen false calls." The idea that eCall could make it harder, not easier, for emergency dispatchers to do their work has been raised as a concern for some time. But Bergonzi stressed that these teething problems are manageable.
Return to Top	

HEADLINE	**04/27 Iconic pen made by blind for military**
SOURCE	**https://apnews.com/d170f66d783c47689296b1eb5201043f/Iconic-pen-used-by-military,-made-by-**

	blind-people-turns-50
GIST	GREENSBORO, N.C. (AP) — Clifford Alexander scoops a handful of black ballpoint pens, drops them into a small box and shakes it with a blackjack dealer's nonchalance. He slides in the next handful to make an exact dozen, and sends the box down the assembly line. Alexander, who is blind, performs the quick act again, box after box. Anyone who's served in the military, worked for the federal government or addressed a package at the post office is familiar with the handiwork. But they might not have realized that all the ubiquitous SKILCRAFT U.S. Government pens were made by the visually impaired. The pens turn 50 this month. The pen's history traces back to April 20, 1968, when it was introduced to government buyers, said the National Industries for the Blind. The nonprofit organization was tapped to supply pens after another manufacturer made 13 million defective ballpoints in 1967. The pens have stringent requirements — 16 pages worth. The pens must be able to write a continuous line 1 mile (1.6 kilometers) long and keep the ink flowing despite extreme temperatures — from 40 degrees below zero to 160 degrees (4 to 71 degrees Celsius). For five decades, the task of making those pens has been entrusted to blind workers. "It may take us longer to learn it, but once we learn those jobs we do those jobs very well," said Alexander, who supervises about 30 Greensboro pen workers. "And we turn out a top quality garment or writing instrument." The pen is well-known among military and government families after finding its way into purses and backpacks for years. It's also been used by the military as improvised devices to plug holes in pipes on boats or perform emergency medical procedures. The pens are sold to the federal government through a program started in 1938 to create jobs for people with disabilities. In 2016, the AbilityOne program sold $3.3 billion in goods and services, with more than half coming from military orders. Alexander said his 47 years at the North Carolina plant has helped him to buy a home and educate his children. The plant employs about 140 visually impaired people to make products ranging from Army combat jackets to clipboards. In the pen's heyday, the government bought about 70 million per year. Now the Greensboro plant and a second in Milwaukee combine to produce about 8 million of the flagship retractable ballpoints annually, with parts supplied by a third site in Missouri. All three employ visually impaired workers. Lynn Larsen, who's worked at Greensboro Industries of the Blind for 40 years, said the job helped her support her family after her father died. More recently, it was a source of pride when her nephew deployed to Afghanistan with the Army. "He would tell the other soldiers that his aunt Lynn made that pen, and they thought it was real cool," she said. The Greensboro workers earn well above minimum wage and can reach around $24 per hour, said Richard Oliver, the site's director of community outreach and government relations. The benefits go beyond the pay, said Oliver, who is legally blind himself: "We didn't get the opportunity to serve in the military ... so this is our way to serve." "It gives our people a really big sense of pride," he said.
Return to Top	

HEADLINE	**04/26 Seattle ties high-record temp for day**
SOURCE	**http://mynorthwest.com/968070/record-temperatures-possible/**
GIST	Seattle tied its record high temperature of 82 degrees for April 26 Thursday and Bellingham hit a new record. Bellingham reached 75 degrees at 4:16 p.m. The previous record high for Bellingham — 74 degrees — was set in 1987. In the past 73 years at Sea-Tac, there have been only 17 days in the month of April where temperatures have reached 80 degrees or higher (including Thursday), according to the National Weather Service. The record high for April 26 in Seattle is 82 degrees, initially set back in 1947. At 1:30 p.m., it was 76 in Everett and 79 in Tacoma. Olympia reached 80 degrees. But brace yourself. A dramatic drop in temperature is expected Friday as winds shift and come in off the ocean. “That’s going to end up dropping temperatures in Seattle almost 15 degrees cooler than what we’re expecting for [Thursday],” Reedy said. Showers return Friday evening and stick around off and on throughout the weekend.
Return to Top	

HEADLINE	**04/26 Russia chided for ‘obscene masquerade’**
SOURCE	**https://www.cbsnews.com/news/russia-syria-opcw-staged-videos-witnesses-chemical-weapons-douma-france-uk/**
GIST	THE HAGUE, Netherlands -- Britain and France denounced on Thursday as a stunt and an "obscene masquerade" a move by Russia to produce Syrian witnesses who Moscow says were filmed in "staged videos" in the aftermath of a reported chemical weapons attack. Russian officials brought the purported witnesses for a briefing Thursday at The Hague headquarters of the Organization for the Prohibition of Chemical Weapons. The development is seen as an effort by Russia to discredit widespread reports of an April 7 suspected chemical weapon attack in the town of Douma near the Syrian capital, Damascus, which killed more than 40 people. The West has blamed the attack on President Bashar Assad's government. Syria and Russia deny the claims. "This obscene masquerade does not come as a surprise from the Syrian government, which has massacred and gassed its own people for the last seven years," said France's ambassador to the Netherlands, Philippe Lalliot. Britain's ambassador, Peter Wilson, said he and other Western allies would not attend the briefing. On Wednesday, OPCW inspectors made a second visit to the town of Douma, collecting samples from a new location that will be sent to designated labs for analysis. The suspected poison gas attack has sparked an ongoing clash of narratives between the West and the governments of Syria and its key ally, Russia. Damascus and Moscow insist there was no chemical weapons attack. Opposition activists and first responders who witnessed the attack in Douma, which was under rebel control at the time, say it was carried out by government forces. Many of the victims suffocated in an underground shelter where they were hiding from government airstrikes, the activists said.

	Following the suspected chemical attack, the United States, France and Britain launched joint punitive airstrikes targeting suspected Syrian chemical weapons facilities on April 14.
Return to Top	

HEADLINE	**04/26 Rwanda official: mass graves discovered**
SOURCE	**http://www.foxnews.com/world/2018/04/26/mass-graves-believed-to-contain-more-than-2000-bodies-discovered-in-rwanda.html**
GIST	KIGALI, Rwanda – Mass graves that authorities say could contain more than 2,000 bodies have been discovered in Rwanda nearly a quarter-century after the country's genocide, and further graves are being sought nearby. The new discovery is being called the most significant in a long time in this East African nation that is still recovering from the 1994 killings of more than 800,000 people. Some Rwandans are shocked and dismayed that residents of the community outside the capital, Kigali, where the mass graves were found kept quiet about them for so many years. "Those who participated in the killing of our relatives don't want to tell us where they buried them. How can you reconcile with such people?" asked a tearful France Mukantagazwa. She told The Associated Press she lost her father and other relatives in the genocide and believes their bodies are in the newly found graves. The discovery of the graves in Gasabo district came just days after Rwanda marked 24 years since the mass killings of ethnic Tutsi and moderate ethnic Hutus. "It is very disturbing that every now and then mass graves are discovered of which the now-free perpetrators never bothered to reveal to bereaved families so that they can get closure," the daily newspaper The New Times said in an editorial this week. "Definitely some very cruel people still live in our midst," it added. Between 2,000 and 3,000 people are thought to be buried in the graves based on the number of area residents who went missing during the genocide, Rashid Rwigamba, an official with the genocide survivors' organization Ibuka, told AP.
Return to Top	

HEADLINE	**04/27 Surging ranks of super-commuters**
SOURCE	**https://www.cbsnews.com/news/the-surging-ranks-of-super-commuters/**
GIST	Coast to coast, Americans commute to work. But one group of commuters stands out from the rest -- and it's getting a larger: super-commuters. These are the people who spend 90 minutes or longer traveling to work, whose numbers surged nearly 30 percent between 2005 to 2016, to 4 million, according to an analysis of U.S. Census data released this week by online rental marketplace Apartment List. Apartment List found the share of super-commuters among the total commuter population rose in 39 states and three-quarters of the largest U.S. metropolitan areas. Eight of the 10 metropolitan areas with the largest share of super-commuters are in the regions surrounding San Francisco, Los Angeles and New York, which have among the country's the highest costs of living "I wasn't surprised that it was high in the San Francisco Bay area or New York or in L.A. because you do hear those stories a lot. But I was surprised it was so common in so many places, especially in places that aren't that large and don't have that bad of traffic like Las Vegas or Cleveland," said Sydney Bennett, senior research associate at Apartment List. "It's a commentary both on the lack of affordable housing and

	the fact that many cities have very little public transportation." Commutes are getting longer for workers overall. According to Apartment List, the share of commuters traveling 24 minutes or less to work daily fell to 55 percent in 2016 from 59 percent in 2005. The share of commuters traveling 25 minutes or more climbed from 41 percent to 45 percent during that same time. Many super-commuters get to work through a combination of driving and public transportation. Often, they take one or more buses or trains. According to Bennett, super-commuters in regions with robust public transportation systems such as New York, San Francisco and Boston depend more on those networks than those with shorter commutes. The mean age for a super-commuter is 43.4 years old, well above 38.4 average age for regular commuters, according to Apartment List. "The reason super-commuters likely skew a bit older is that those looking for more space (for example, a single-family home versus an apartment with three roommates) while on a tight budget may need to live further from downtown job centers," Bennett said. The super-commuter problem is being exacerbated, she added, because much of the new housing being built is on the periphery of cities that lack robust public transit as opposed to closer suburbs. Many units in downtown areas are geared toward the luxury market, squeezing out low-income residents. "For these displaced residents, improved transit provides easier access to job centers and offers improved social mobility," the report says. In the time since the Census data was released, Bennett argues that the circumstances affecting super-commuters haven't changed much. "Anecdotally," she said, "we're hearing that it's either the same or worse in the last year-and-a-half."
Return to Top	

HEADLINE	**04/25 Arctic ice record amount of plastic**
SOURCE	**https://www.usatoday.com/story/news/world/2018/04/25/arctic-ice-choked-record-amount-microplastic-cigarette-butts-packing-material/549115002/**
GIST	If you are wondering what happens to all those cigarette butts flicked on sidewalks and plastic packing peanuts blowing down the street, researchers have found an alarming amount of particles from them deep in the ice of the Arctic Ocean. The record amount of microplastic appears to be courtesy of the Great Pacific Garbage Patch and increased fishing and shipping in the Arctic, researchers at the Alfred Wegener Institute of the Helmholtz Center for Polar and Marine Research report. The study raises concerns about the impact on human and sea life. Ice samples from five regions across the Arctic Ocean contained up to 12,000 of the tiny particles per liter of sea ice, researchers say. More than half the particles trapped in the ice were less than 1/500th of an inch wide — less than one-tenth the thickness of a credit card. “They could easily be ingested by arctic microorganisms,” said biologist and report author Ilka Peeken. “No one can say for certain how harmful these tiny plastic particles are for marine life, or ultimately also for human beings.” Microplastic refers to plastic particles, fibers, pellets and other fragments with a length, width or diameter ranging from microscopic to two-tenths of an inch.

	The types of plastic showed a "unique footprint" in the ice allowing the researchers to trace them back to possible sources. Some can be traced to the Great Pacific Garbage Patch, a collection of plastic, floating trash halfway between Hawaii and California, that has grown to more than 600,000 square miles, the report says. Researchers determined that ice floes contain particularly high concentrations of polyethylene, used primarily in packaging material. "We assume that these fragments represent remains of the so-called Great Pacific Garbage Patch and are pushed along the Bering Strait and into the Arctic Ocean by the Pacific inflow," the study says. A high percentage of paint and nylon particles pointed to the intensified shipping and fishing activities in some parts of the Arctic, the study says. The researcher team gathered the ice samples during three expeditions in 2014 and 2015. The study was released in the journal Nature Communications.
Return to Top	

HEADLINE	**04/26 JFK documents: Oswald's KGB handler**
SOURCE	**https://www.newsmax.com/newsfront/lee-harvey-oswald-kgb-handler-jfk-assassination/2018/04/26/id/856981/**
GIST	One of the 19,045 CIA and FBI documents on President John F. Kennedy's Nov. 22, 1963, assassination released Thursday revealed the "KGB handler" of gunman Lee Harvey Oswald. According to McClatchy, the documents fill in some blanks about a Soviet Embassy official in Mexico City who met with Oswald weeks before the assassination. Over the decades, Oswald's meetings in Mexico City with the Cuban and Soviet embassies, purportedly to get a visa to Cuba in hopes of returning to the Soviet Union, have gradually been revealed, McClatchy reported. But the Thursday release revealed one of the Soviets he had contact with was Valeriy Vladimirovich Kostikov. McClatchy reported the CIA confirmed to the original assassination investigators that Kostikov was likely part of the Department 13 assassination unit of the Soviet spy agency, the KGB. It is now known Oswald had phone conversations while in Mexico with Kostikov — and among the further-released documents Thursday were references to Kostikov being "Oswald's KGB handler." It is found in a May 1982 memo from what appears to be an unidentified foreign intelligence agency or U.S. asset in the Middle East asking longtime CIA Soviet Division leader David Blee about Kostikov. The questioner notes the Soviets were behind increased harassment of foreign embassies in Beirut – less than a year before a truck bomb leveled the U.S. embassy there, killing 241 U.S. marines and military personnel. "The reason for our interest in KOSTIKOV will be obvious," writes the official to Blee. That document was one of more than 15,000 that Thursday were left with some form of partial redaction. Another document released Thursday revealed a memo dated Sept. 30, 1963, revealing FBI field agent James Hosty Jr. had sent word back to headquarters on the activities of Oswald.

	The document makes clear Hosty did tell FBI bosses Oswald was violent and had been living and working as a maintenance man in New Orleans before moving to Dallas in the spring of 1963. And it confirms Oswald was under surveillance at the time of the assassination. The agencies have until Oct. 26, 2021, to fully lift the veil of secrecy on the documents about the assassination – almost 58 years after the events in Dallas.
Return to Top	

HEADLINE	**04/26 Dark chocolate gives brain a boost?**
SOURCE	**http://abcnews.go.com/GMA/Wellness/dark-chocolate-give-brain-boost-studies-suggest/story?**
GIST	Here's a reason not to feel so guilty about indulging in your afternoon chocolate fix. Dark chocolate may be giving your brain, immune system and eyes a real boost. This week, researchers brought out three new studies singing the praises of this delectable treat. Scientists in one study allowed lucky volunteers to eat one dark chocolate bar, about 1.5 ounces, and then studied their brain waves with a machine called an E.E.G. Researchers found an increase in gamma waves 30 minutes after eating the chocolate. "Gamma frequency is associated with neurosynchronization, in other words neuroplasticity.... It is the highest level of cognitive processing," Dr. Lee Burk, the principal investigator of this study, explained. Neuroplasticity describes the brain's ability to efficiently connect thoughts and ideas. Scientists believe that gamma waves are a sign that your nerve cells are firing on all cylinders. They are able to talk to each other in a manner that leads to optimum learning and memory formation. Immunity booster In another study, Burk looked at how dark chocolate affects the immune system. Again, participants ate a dark chocolate bar, and scientists studied their blood work for the following week. They found an increase in anti-inflammatory markers as well as an increase in T cells, infection-fighting cells. These findings are overall "great for immunity," according to Burk. It's important to know that both of these studies were very small, with only 10 blessed participants. Not to mention, these results were presented at a scientific meeting, not published in a journal, which means they were not highly scrutinized, or "peer-reviewed," before they were revealed. A dark chocolate vision boost But another study was published in JAMA Ophthalmology, a journal produced by the American Medical Association. In two different tests, they gave 30 participants two chocolate bars, both dark and milk chocolate, and conducted vision tests about two hours later. After eating dark chocolate, the participants had small improvements in their vision. The most significant: improvement in contrast sensitivity, meaning your ability to tell the difference between objects in a low light or high-glare setting. In real life, contrast sensitivity comes into play when driving at night, for example. It is unclear why dark chocolate affects vision; however, the authors think it has to do with the blood vessels in the eye. Cacao, the main ingredient in dark chocolate, has been shown to positively affect blood pressure and blood vessel function. This new research suggests that dark chocolate allows for more blood flow to back of the eye, therefore improving vision. But make sure it's really dark -- 70 percent cacao

	Before you gorge yourself on brownies and hot fudge sundaes in the name of science, all of these studies are very specific to dark chocolate. Researchers used dark chocolate with 70 percent cacao, a recipe reserved for the darkest of dark chocolate. This usually means the chocolate tastes more bitter than sweet because only 30 percent of the candy bar is sugar and milk. "It's really not a candy," Burk said of the chocolate used in his study. "It's the sugar that's a candy, not the cacao."
Return to Top	

Crime, Criminals

Top of page

HEADLINE	**04/26 Police: explosive device Texas Starbucks**
SOURCE	**http://www.12newsnow.com/article/news/crime/police-legitimate-explosive-device-inside-suspicious-package-found-at-beaumont-starbucks/502-545979304**
GIST	Beaumont Police now say they believe a "legitimate explosive device" was found early Thursday morning at the Dowlen Road Starbucks location. The suspicious package which contained the device was "rendered safe" by bomb technicians from the FBI and the Bureau of Alcohol, Tobacco, Firearms and Explosives according to a release from the Beaumont Police Department. The Port Arthur Fire Department EOC K-9 assisted according to the release. The package was discovered at the Starbucks in the 3900 block of Dowlen Road near the Kroger grocery store. A spokesperson for the Bureau of Alcohol, Tobacco, Firearms and Explosives told 12News that the "device could have caused harm if detonated properly." Police confirmed in the release that a note was found in the package but did not disclose what it said. A Starbucks employee who asked to remain anonymous told 12News that a note found inside the package read "Die U.S.A." The package, which was initially found outside the Starbucks, was brought inside by an employee according to the release. The employee noticed the note when they attempted to open the package and then put it back outside and called police. Police were called at about 4:45 a.m. and closed Dowlen Road near Folsom for almost three hours. Employees told police the package had been at the store for a few days.
Return to Top	

HEADLINE	**04/26 Virginia top court curtails police ALPR use**
SOURCE	**http://www.nbc29.com/story/38054562/va-supreme-court-delivers-blow-to-police-use-of-license-plate-reader-technology**
GIST	RICHMOND, Va. — The Virginia Supreme Court has delivered a blow to the police's use of Automated

	License Plate Readers (ALPRs) to surveil citizens and track drivers' movements. The Rutherford Institute filed an amicus brief in Neal v. Fairfax County Police Department challenging the police practice of collecting and storing ALPR data as a violation of Virginia law that prohibits the government from amassing personal information about individuals, including their driving habits and location. In reversing a lower court ruling that allowed state law enforcement agencies to extend the government's web of surveillance on Americans by tracking them as they drive their cars, the Court held that the use of ALPRs involves the collection of personal information prohibited by Virginia's Government Data Collection and Dissemination Practices Act. Mounted next to traffic lights or on police cars, ALPRs, which photograph up to 3,600 license tag numbers per minute, take a picture of every passing license tag number and store the tag number and the date, time, and location of the picture in a searchable database. The data is then shared with law enforcement, fusion centers and private companies and used to track the movements of persons in their cars. The Virginia Supreme Court's opinion in Neal v. Fairfax County is available at www.rutherford.org. "We're on the losing end of a technological revolution that has already taken hostage our computers, our phones, our finances, our entertainment, our shopping, our appliances, and now, it's focused its sights on our cars," said constitutional attorney John W. Whitehead, president of The Rutherford Institute and author of Battlefield America: The War on the American People. "By subjecting Americans to surveillance without their knowledge or compliance and then storing the data for later use, the government has erected the ultimate suspect society. In such an environment, there is no such thing as 'innocent until proven guilty.'" Since 2010, the Fairfax County Police Department (FCPD) has used ALPRs to record the time, place, and driving direction of thousands of drivers who use Fairfax County roads daily. License plate readers capture up to 3,600 images of license tag numbers per minute and convert the images to a computer format that can be searched by tag number. This information, stored in a police database for a year, allows the police to determine the driving habits of persons as well as where they have been. In 2014, Fairfax County resident Harrison Neal filed a complaint against FCPD asserting its collection and storage of license plate data violates Virginia's Government Data Collection and Dissemination Practices Act (Data Act), a law enacted because of the fear that advanced technologies would be used by the government to collect and analyze massive amounts of personal information about citizens, thereby invading their privacy and liberty. The lawsuit cited a 2013 opinion by Virginia Attorney General Ken Cuccinelli that ALPR data is "personal information" that the Data Act forbids the government from collecting and storing except in connection with an active criminal investigation. Despite this opinion, FCPD continued its practice of collecting and storing ALPR data in order to track the movements of vehicles and drivers. In November 2016, a Fairfax County Circuit Court judge ruled that license plate reader data was not "personal information" under the Data Act because license tag numbers identify a car and not a person. The Virginia Supreme Court reversed that decision, ruling the data was personal information, and remanded the case for a determination of whether the ALPR record-keeping process allows a link to be made between the license plate number and the vehicle owner.
Return to Top	

HEADLINE	**04/27 Privacy fears over 'genetic informants'**
SOURCE	**https://www.apnews.com/de2a1166d5664125858cb7b5eed209a5/Use-of-DNA-in-serial-killer-probe-sparks-privacy-concerns**
GIST	SACRAMENTO, Calif. (AP) — Investigators who used a genealogical website to find the ex-policeman they believe is a shadowy serial killer and rapist who terrified California decades ago call the technique

	ground-breaking. But others say it raises troubling legal and privacy concerns for the millions of people who submit their DNA to such sites to discover their heritage. There aren't strong privacy laws to keep police from trolling ancestry site databases, said Steve Mercer, the chief attorney for the forensic division of the Maryland Office of the Public Defender. "People who submit DNA for ancestors testing are unwittingly becoming genetic informants on their innocent family," Mercer said, adding that they "have fewer privacy protections than convicted offenders whose DNA is contained in regulated databanks." Joseph James DeAngelo, 72, was arrested Tuesday after investigators matched crime-scene DNA with genetic material stored by a distant relative on an online site. From there, they narrowed it down to the Sacramento-area grandfather using DNA obtained from material he'd discarded, Sacramento County District Attorney Anne Marie Schubert said. Authorities declined to name the online site. However, two of the largest, Ancestry.com and 23andMe, said Thursday that they weren't involved in the case. DNA potentially may have played an earlier role in the case. It was just coming into use as a criminal investigative tool in 1986 when the predator variously known as the East Area Rapist and the Golden State Killer apparently ended his decade-long wave of attacks. DeAngelo, a former police officer, probably would have known about the new method, experts said. "He knew police techniques," said John Jay College of Criminal Justice professor Louis Schlesinger. "He was smart." No one who knew DeAngelo over the decades connected him with the string of at least a dozen murders, 50 rapes and dozens of burglaries from 1976 to 1986 throughout the state.
Return to Top	

HEADLINE	**04/26 Texas church shooter promised judge**
SOURCE	**http://time.com/5256917/sunderland-springs-texas-shooter-devin-kelley/**
GIST	(AUSTIN, Texas) — The gunman in a mass shooting at a Texas church last year told a military judge in 2012 he "would never allow myself to hurt someone" again while admitting to abusing his stepson and a long struggle with anger, according to Air Force records obtained by The Associated Press on Thursday. The documents and transcripts offer a rare look at Devin Patrick Kelley speaking at length and in his own words, as few examples have previously surfaced in the six months since he opened fire during a Sunday service in tiny Sutherland Springs, Texas. Kelley killed more than two dozen people in November 2017 in the worst mass shooting in Texas history. He died of an apparent self-inflicted gunshot wound after he was shot and chased by two men who heard the gunfire at the church. "I don't think adults change. I don't think people change," Kelley said during his court-martial at Holloman Air Force Base in New Mexico, according to a transcript. He was convicted of assaulting family members and ultimately given a bad conduct discharge. "I believe in miracles. I believe in angels and I believe in demons, but I think for most people, they're going to be who they are and live their lives out, but based on the choices they make, if they're a wife beater, they're gonna probably beat their next wife. If they're a child beater, they'll probably beat their

	own child." The AP obtained hundreds of pages surrounding Kelley's court martial through a Freedom of Information Act request. Kelley admitted to pushing his stepson while the toddler crawled on the floor and slapping him across the face when he wouldn't stop crying. He cracked the child's skull and broke his clavicle. His ex-wife wrote an affidavit that described in graphic detail how Kelley repeatedly hit her, choked her and twice pointed a gun at her. She wrote that when she suggested they get a divorce during a drive, Kelley lost control of their car while grabbing her hair, causing them to strike a guard rail. "Sir, this is the worst thing I've done in my life and I will never allow myself to hurt someone like this again," Kelley said. Five years later, Kelley went aisle to aisle at the First Baptist Church in Sutherland Springs looking for victims. Witnesses said he shot crying babies at point-blank range and the dead ranged in age from 18 months to 77 years old. Authorities put the official death toll at 26 because one of the 25 people killed was pregnant. Investigators have said the attack appeared to stem from a domestic dispute Kelley was having with his mother-in-law, a member of the church who wasn't present that day. Air Force prosecutors had pushed for a stiffer sentence than the 12 months confinement and bad conduct discharge that Kelley received from the military jury. They wanted four years of prison time so that he might get his anger under control, according to the trial transcript. "Who's next?" said Capt. Brett Johnson, the assistant trial counsel. "What are we going to do to ensure that this does not happen again? That the next time he lashes out in anger to strike a child, to choke a woman, let him think back to the four (years) he sat in confinement, then maybe he will think again." The records show Kelley struggled to comply with the exacting standards of military service. A May 2012 evaluation rated his performance as an airman first class "average" and noted that he'd received letters of reprimand for insubordination to a superior enlisted service member and an assault on a family member. Kelley did not meet the requirements for conduct, character and military bearing, according to the evaluation. After a confrontation with a civilian colleague over work duties, Kelley described being "scared and holding back tears" when the person yelled and tried to intimidate him, according to his summary of the incident, which is among the documents released. The civilian wanted to settle the dispute immediately in front of a staff sergeant, but Kelley said he needed time to get control of his emotions. During the court-martial, Kelley submitted pictures of him in Boy Scouts, handling pets on his family ranch and rock-climbing with his family. He described being bullied on the football team in high school, hiding "behind alcohol and self-denial" and considering suicide before reconnecting with God. "It will take a lifetime of living up to the promises I've made to myself, God and here to prove I have changed," Kelley wrote in an affidavit. "I know I can be better, I just need a chance to prove it."
Return to Top	

HEADLINE	**04/26 Everett mayor, PD chief eye gang violence**
SOURCE	**http://mynorthwest.com/968301/everett-mayor-police-chief-tackling-gang-violence-head-on/**
GIST	Everett's new mayor announced a new plan to tackle youth gang violence after a significant increase last

year.

Police Chief Dan Templeman says they've noticed a steady increase in gang and gun violence for a couple of years, everything from graffiti and tagging to drive-by shootings.

But it got really bad in 2017 with an increase in shootings overall and a 75 percent jump in gang-related crimes in the first 10 months of the year, most committed by people under 21.

In October 2017, 14-year-old Mariner High School Freshman David Sandoval was shot and killed by a 13-year-old boy over the color of his shoes.

"Anytime you have 13-year-olds that are armed with weapons and guns and they're using them to commit crimes, I mean that's as a police chief, it's completely unacceptable," said Chief Templeman. "In my mind, we needed to do something."

Templeman met with Sandoval's dad, and others living in the area as well as community groups around the Casino Road area and south Everett where many of the shootings and gang issues were happening.

"And it really brought to light the situation out there and the conditions and some of the fear that the community was feeling last year," said Templeman. "And so it allowed me to really take a look at our organization and how we were deploying our resources and make some adjustments in how we were deploying our police officer resources."

He was hearing from people in these communities who were afraid to let their kids walk to school, play outside of their homes, or go to the store.

Late last year, Templeman started directing extra patrols in the areas where guns, gangs, and youth violence had been a problem. And in recent months, the chief dedicated a sergeant and four officers to work with gangs and engaging with communities.

In January, newly-elected Mayor Cassie Franklin made addressing the issue of gun and gang violence involving young people a priority, issuing a directive for a more wide-ranging plan that includes several initiatives.

"They really represent a holistic approach to this and it's not just focusing on enforcement and it's not just focusing on prevention and intervention or public education," said Templeman. "It really looked at this issue from a big picture perspective … not treating the symptoms of the problem, but really trying to treat the disease and get at that."

He says it's a similar approach to efforts being used to fight the opioid crisis.

Among the new initiatives is the creation of a Gang Response Community Advisory Group. The group was formed earlier this year and has met several times. Among the members, Sandoval's dad, police, community groups and community members, including students who have had to deal with gangs.

Templeman says in the weeks ahead they'll be taking more steps on the prevention front.

"Enforcement is important and we are right still examining and evaluating organizationally the feasibility and the likelihood of standing up our own Gang Response Unit in the city of Everett that would be dedicated — a group of officers," said Templeman. "It would also include a prevention and education component as well so not just enforcement, but a team of enforcement officers that can go out and work in the communities in the areas that are being hit."

Templeman says those prevention and intervention tools are an essential tool, especially when many kids getting involved in gangs have parents or siblings who are already involved or have little parental supervision.

	The Firearms Safety Program will offer free gun locks and partner with local gun shops to provide information about the dangers of not safely storing guns when they sell a gun. "We see firearms stolen a lot in the city of Everett," said Templeman. "We see firearms stolen out of vehicles. They're beneath the driver seat, they are in a backpacks, they're under a blanket in the back seat. We see firearms stolen in burglaries at people's homes where the firearm is sitting on the night stand. Our big concern about that is that those firearms end up in the hands of the wrong people. They end up in the hands of criminals. They end up in the hands of children." Templeman says the goal is to have the Gang Response Unit and Firearms Safety program up and running sometime in June 2018. In the meantime, things are looking up for the first part of this year with gang crimes down 59 percent in the first three months of 2018 compared to the same time in 2017. Templeman said, "Our shootings are down 37 percent in the city of Everett, our drive-by shootings are down 87 percent in the first quarter compared to last year. So trending in the right direction." The chief is cautiously optimistic, but warns gang activity usually increases in the summer months.
Return to Top	

HEADLINE	**04/26 Violent rivals rush into FARC void**
SOURCE	**https://www.reuters.com/investigates/special-report/colombia-peace/**
GIST	Despite government efforts to bring order to Colombia, police and military forces are now struggling against various armed groups vying for land and illegal activities once controlled by the Revolutionary Armed Forces of Colombia, or FARC. Still a powerful criminal enterprise when it agreed to demobilize, the FARC left behind lucrative dealings in the drug trade, extortion and illegal mining. Stepping in to supplant them are splinter FARC factions, enterprising new gangs and veteran rebel rivals like the National Liberation Army, or ELN. Reuters accompanied soldiers, police, guerrillas and townspeople to understand the difficulties still confronting Colombia. When President Juan Manuel Santos and leaders of the Revolutionary Armed Forces of Colombia shook hands to end a half-century war, residents of towns like Tumaco were supposed to be relieved. Nineteen months later, people in this gritty port on the Pacific are anything but. True, most FARC militants, as foreseen by the peace accord, demobilized here and across Colombia, a country the size of France and Spain combined. For decades, rugged terrain and an oft-absent government had enabled the rebels to become the de-facto authority in many areas. But Santos, saddled with a sluggish economy at the end of his second term, has struggled to ensure order of the sort the rebels, albeit murderous, once imposed across parts of the Andean nation. Despite widespread acclaim for the agreement, including a Nobel Prize for Santos, peace remains elusive in this country of 50 million people, still the world's largest producer of cocaine. With the FARC disarmed, other militants, criminal gangs and paramilitary groups are jostling into the breach. They are hoisting flags, enlisting members and exacting levies and loyalty in former FARC strongholds. They are also seizing the FARC's most lucrative rackets – from the drug trade, to extortion, to illegal mining.

"It's like a devil's cauldron where all manner of criminal ingredients are being boiled," said Juan Camilo Restrepo, until recently the government's chief negotiator in ongoing peace talks with the National Liberation Army, or ELN, now Colombia's biggest guerrilla group. "They all want their hands on the business and territorial spoils left by the FARC."

Over the past nine months, Reuters traveled to Tumaco and six other sites in Colombia to understand the advance of armed and criminal groups. Disrupters include splinter FARC factions, enterprising new gangs and veteran rebel rivals, like the ELN, who have used the agreement to reposition.

Among the most violent corners of Colombia is Tumaco, in the southwest, where a network of rivers provides a crucial Pacific outlet for sprawling coca plantations nearby.

Here, new guerrilla corps vie with criminal gangs for the routes. Earlier this month, a small force of former FARC fighters killed an Ecuadorian journalist, photographer and their driver because the neighboring country spurned the guerrillas' demands that it release imprisoned comrades who had ventured across the border.

East of Tumaco, ELN rebels seized turf where the FARC relinquished an illegal gold mine. In the northwestern state of Chocó, the ELN is recruiting and expanding control of jungle there.

To win support for the deal, Santos promised to flood areas of FARC control with troops and investment.

As much as $3 billion of annual government spending over the next 15 years is supposed to improve health, education, infrastructure and agriculture in war-torn regions. A cornerstone of the plan is a crop substitution effort for farmers who rely on income from coca.

But a weakened economy makes financing difficult.

Along with tighter budgets, red tape delays the start of roads, aqueducts, schools, power lines and clinics promised to millions living without infrastructure. The crop substitution program in 2017 reached just 30 percent of its goal and is angering farmers who say the government is leaving their fields bare. The anger boiled over near Tumaco in October, when seven farmers died in a firefight with police and soldiers who pulled up their coca bushes.

The ascendant threats are dividing Colombians just before they vote on a Santos successor in May. Instead of an asset, the faltering peace is disconcerting an electorate also frustrated by tepid growth, weak public services and still-gaping inequality.

The government said it is doing all it can.

It already deployed 80,000 police and soldiers. In January, it launched its biggest deployment in two decades, sending 9,000 troops to Nariño, the troubled state home to Tumaco and other flashpoints along the Pacific coast and Ecuadorian border.

It isn't enough.

Groups such as the new and little-known United Guerillas of the Pacific are establishing strongholds. "This is happening all across Colombia," said Joan, the leader of an eight-person squad of heavily-armed guerrillas on patrol late last year in jungle south of Tumaco.

Led by former FARC fighters who rejected the peace, the group is already coercing local families for support. It is not associated with the rebels who killed the Ecuadorians earlier this month, according to government officials.

Luis Carlos Villegas, Colombia's defense minister, told Reuters the problems with other gangs, guerrillas and criminals aren't new or worsening. Rather, he argued, they stand out in the void left by the FARC.

"Are there micro-trafficking problems? Are there organized crime problems? Are there problems of gangs that are trying to move into FARC territories?" Villegas asked. "Yes."

"But are they growing?" he continued. "No, they are more visible because there is no longer a conflict."

As many as 70 armed and criminal groups operate across Colombia, according to Ariel Ávila, a researcher at Fundación Paz y Reconciliación, a security think tank in Bogotá, the capital. That amounts to about 5,000 guerrillas, gang members, paramilitary fighters and other criminals, including FARC dissidents who renounced the peace.

In a briefing in late March, General Alberto José Mejía, Colombia's top military commander, said as many as 1200 FARC dissidents are still active, one fifth the rebel force when peace was agreed. While a far cry from the 17,000 rebels at the FARC's peak in the late 1990s, the figure is four times the number the government had previously recognized.

Some dissidents have set up splinter factions, like the Pacific guerrillas, who are already "taxing" local traffickers and extorting grocery stores and other small businesses. Police believe extortion fuels as much as 20 percent of the income for some groups.

Other dissidents joined gangs with little ideology beyond crime.

The FARC originated in the 1960s, a leftist insurgency against the government and an entrenched elite who even today control most of Colombia's resources. Initially inspired by communism, the FARC diversified into kidnapping, extortion, the drug trade and other crimes as Cold War credos faded.

For those who now seek to supplant them, there are many opportunities for ill-gotten gains. The resulting turf wars and violence perpetuates one problem, the displacement of noncombatants from homes and entire communities, that totalled more than 67,000 people last year, according to Colombia's government.

Around Tumaco, where wood and tin shacks rise on stilts above meandering estuaries, the scramble for control spawned bloodshed. Many of its 200,000 residents, most of African and indigenous descent, miss the days before the agreement.

Back then, the FARC controlled local drug routes. Despite frequent clashes with government troops, the rebels ensured that most poor residents and non-combatants were left alone. Today anyone is vulnerable.

Nationwide, murders have declined in recent years. In Tumaco, and other former FARC bastions, homicides are soaring.

At least 211 people were killed in Tumaco last year, according to police, compared with 147 in 2016. That gives Tumaco a homicide rate of about 102 murders per 100,000 people – roughly four times the national rate.

For townspeople in Tumaco, poverty can make life outside the law attractive. City hall calculates unemployment at 70 percent. Few legitimate jobs exist beyond seasonal work on shrimp boats, other fishing and farming of cacao, rice and palm.

The easiest money, then, is cocaine – be it coca cultivation or any of the chemical or logistical activities to export it. Across Colombia, such activities generate about $13 billion annually, according to government estimates, equal to more than 4 percent of the country's legitimate economy.

In Tumaco's muddy slums, youth idle on street corners, drinking beer and listening to reggaeton music. Some are awaiting recruitment by local gangs for one lucrative activity – running cocaine in high-speed boats to Central America.

Gangs own or rent the boats, with outboard motors powerful enough to carry as much as three tons to dropoff points in Panama, Costa Rica or beyond. For each voyage, they pay roughly 100 million pesos, or about $35,000, to each runner in a crew of three or four.

Sometimes, the voyages are multi-party enterprises, with small businesses and others investing. Even those meant to thwart the trade, including sailors at checkpoints, sometimes get a cut in exchange for turning a blind eye, locals and police said.

Bribes are a constant challenge, particularly because drug profits allow criminals to pay more than the state.

“They use their abundant capital to corrupt institutions,” said Orlando Romero, the admiral in charge of operations on the Pacific. The Navy, he added, arrested 12 sailors over the past three years for collaborating with drug runners.

The voyages from Tumaco are hardly new. But the rush to participate has accelerated.

“They come to church for blessing before they go,” said Daniel Zarantonello, an Italian priest in Tumaco. “It’s out of control.”

Farmers are also growing more coca.

The region around Tumaco is now Colombia’s biggest source of the leaf.

Some 23,000 hectares, over three times the area of Manhattan, are planted there, according to the U.S. Drug Enforcement Administration. Cultivation nationwide reached 188,000 hectares in 2016, over twice the area three years earlier.

The increase has various causes, including Colombia’s 2015 decision, for health and environmental reasons, to stop aerial dusting of pesticide on coca plantations. The FARC also sought to maximize cocaine revenues before demobilizing.

The result: Cocaine production capacity reached 910 metric tons in 2016, the highest in over a decade, according to DEA figures.

In Peña de los Santos, a hamlet four hours south of Tumaco by boat on the Rosario River, farmers grow coca and make it into paste. For a spell after the peace agreement, buyers no longer came. Many in the Afro-Colombian community had to scrounge for fruit and fish.

For many farmers, little incentive exists to grow crops the government hopes can blossom through substitution.

A hectare of coca, a fast-growing plant that can be harvested in three months, can reap 44 million pesos a year, about $15,000, according to national police in the area. A hectare of cacao, the slow-growing source of chocolate, generates a tenth as much.

Return to Top

HEADLINE	04/26 Inmate bought mail bomb off dark web
SOURCE	https://www.upi.com/Top_News/US/2018/04/26/SC-inmate-bought-mail-bomb-off-dark-web-to-kill-ex-wife/9091524711151/?utm_source=fp&utm_campaign=lh&utm_medium=5
GIST	April 25 (UPI) -- A South Carolina prisoner was convicted this week of using the dark web to sell drugs and obtain a mail bomb to be sent to his ex-wife. Michael Young Jr., 32, was already serving a 50-year sentence for attempting to kill his ex-wife and

	murdering her father back in 2007 when he got a hold of a contraband cell phone he used to access the dark web and carry out his crimes. Prosecutors said he used the phone to purchase marijuana via a supplier in California that was sent to a residence in South Carolina, where Young's co-conspirator, Vance Volious Jr., would pick it up and re-distribute it. Several other people have also been implicated in the drug conspiracy, including 14 South Carolina Corrections Department officers who were indicted Wednesday. But Young didn't stop with the drug dealing. He also wanted to finish kill the woman he attempted to kill more than a decade earlier. "Let me ask you this...could u possibly booby trap a box? So that as soon its opened...boom? Just curious," Young wrote to a seller on the dark web's Alpha Bay Market. The seller said it could be done and Young sent cryptocurrency to pay for the "box." "Young used Bitcoin to pay for the mail bomb to be sent to a conspirator's residence," prosecutors said. "He also had re-shipment labels addressed to his ex-wife to be sent to Volious' house in Columbia. Co-conspirator Tyrell Fears -- who previously pleaded guilty -- obtained the labels from Volious, armed the mail bomb and delivered the inert explosives package to the Post Office in [Irmo, S.C.] on June 6, 2017." The mail bomb might have been delivered if a U.S. Postal Inspector didn't intercept the package. The next day, Young, Volious and Fears were indicted. Young and Volious were both convicted of conspiracy, transport of an explosive with the intent to kill, mailing a non-mailable explosive with the intent to kill, and carrying an explosive during the commission of another felony.
Return to Top	

HEADLINE	**04/26 German nurse faces 98 murder charges**
SOURCE	**http://abcnews.go.com/International/wireStory/german-nurse-faces-murder-charge-total-rises-98-54746606?cid=clicksource_76_2_hero_headlines_headlines_hed**
GIST	German prosecutors have attributed one more murder to a former nurse accused of killing dozens of patients at two hospitals, bringing to 98 the number of slayings he is expected to face trial for later this year. Niels Hoegel is already serving a life sentence for two murders. He was charged earlier this year with killing 97 more patients over several years at the hospitals in northwestern Germany. His trial is scheduled to open Oct. 30 in Oldenburg. News agency dpa reported that prosecutors said Thursday they are accusing Hoegel of one more killing after medical experts found traces of a cardiac drug in samples from one patient but erroneously told investigators the result was negative. The state court will decide whether to add the case to the indictment.
Return to Top	

HEADLINE	**04/25 Vehicle rental agencies safety concerns**
SOURCE	**https://www.theglobeandmail.com/canada/article-vehicle-rental-agencies-struggle-with-screenings-as-security-concerns/**
GIST	Monday’s deadly rental van rampage in Toronto shows how quickly a vehicle can be turned into a weapon, but rental agencies are finding few clear options to prevent their property from involvement in such violent acts.

The urgency to find solutions is increasing, however.

The attack in Toronto that left at least 10 people dead and several injured is only the latest of a spate of vehicle attacks — including one in Edmonton last September — that have security experts grappling with solutions.

Efforts are further along in Europe, which has seen a rash of vehicle attacks across the continent. In the U.K., vehicle rental companies were asked to conduct tougher background checks following two separate van attacks in London last June.

But rental agencies are still limited in how well they can screen customers, said Toby Poston, director of communications at the British Vehicle Rental and Leasing Association.

“Members aren’t experts at profiling customers,” said Poston.

“People don’t come into rental branches wearing camo gear and stab vests and with that sort of glint in their eye. Quite often, these people just present themselves like any normal person.”

The British association is, however, looking to better co-ordinate with law and security officials to make it easier to share data. Poston said rental agencies wouldn’t have access to terror watchlists or the like, but could potentially feed information to authorities for better monitoring.

Member companies are also looking to potentially institute other record searches like credit and criminal background checks, but even then there is no clear way to determine that a vehicle shouldn’t be rented, said Poston.

“You have to remember that a criminal record is not always reason enough to not rent someone a vehicle. And you have to be careful from a discrimination point of view.”

The accused in the Toronto van attack, Alek Minassian, did not even raise any red flags during a brief stint in the Canadian Armed Forces last year, a military source told The Canadian Press.

Toronto police said he rented the van from a Ryder rental location north of the city. The company said Tuesday it was fully co-operating with authorities, but declined to comment on its current security policies.

The Associated Canadian Car Rental Operators said government officials have yet to reach out to try to co-ordinate data sharing.

But any such efforts would be complicated, said vice president of government relations Craig Hirota.

“It’s challenging, how do you use that information so that it doesn’t infringe on existing rights of the individual and rights to privacy?”

The RCMP’s National Critical Infrastructure Team has been in contact with industry and sends out relevant information, Hirota added.

“We are in the loop with local and federal law enforcement when there are bulletins.”

He said the rental industry has long been concerned with fraudulent and criminal activity with rentals, but there are limited options for screenings.

“Vehicle rental agencies have been concerned with people doing bad things with rental cars since the inception of the industry. Obviously if there was a way to tell a renter was going to do something prohibited with your vehicle, we’d love to have that.”

	The U.K. rental association is looking to security models elsewhere, including the New York Police Department's Operation Nexus program that facilitates reporting of suspicious business encounters. It is also considering the establishment of a national accreditation scheme that could include training and formalizing policies such as no cash rentals. Companies also generally require business accounts for customers wanting to rent larger trucks, said Poston. Elsewhere in Europe, Italy has implemented a real-time notification scheme with rental operators and a similar one is being developed in Belgium. Sweden is looking to introduce geofence technology that could connect with a vehicle's on-board computer and limit its speed to a safe level. The ease of carrying out such attacks, and the difficulties in detecting them are part of the reason for their rise, said Jeremy Littlewood, an assistant professor at Carleton University's Norman Paterson School of International Affairs. "It's easy to replicate if someone gets that into their head," said Littlewood. Littlewood also questioned the effectiveness of background checks. He pointed out that Alek Minassian, now charged with 10 counts of first-degree murder for Monday's attack, was not known to police. "So far, police authorities are saying this person was not known to us. And so even if we had a database, our individual in this case is not going to show up from the police side." Even when perpetrators are known it is still difficult to stop an attack, said Littlewood, noting that Martin Couture-Rouleau was reported to be under RCMP surveillance when in 2014 he used a vehicle in Saint-Jean-sur-Richelieu, Que., to hit two members of the Canadian Armed Forces, leaving one dead. Prevention has instead focused on more cement barriers, and heavy trucks at intersections for major events, but there's no way to fully prevent this sort of attack entirely, said Littlewood. "We have to recognize the limits of what can be done here, and the reality is we have to accept there are going to be some risks, and we can never entirely make ourselves into a zero-risk world."
Return to Top	

HEADLINE	**04/26 Ferry terminals: cut in line, get a fine**
SOURCE	**http://komonews.com/news/local/cut-in-line-get-a-fine-at-state-ferry-terminals**
GIST	EDMONDS, Wash. - Ferry riders beware - as new warnings are out about the crackdown on cutting in line to board a boat. It takes an eagle-eye to catch all the line cutters, and whether it is by accident or on purpose, people keep finding ways to bypass the toll booths and other drivers. "When you deal with the public you're going to find all these people who try to find loopholes in the system," said Rory Rodriguez, a terminal attendant in Edmonds for the Washington State Ferries. Peer pressure keeps most passengers honest. However, even drivers who sneak in a shortcut don't always do it intentionally. "People are guided by GPS, and GPS doesn't always pick up where the back is at and where a queue or a line for the ferry starts or ends," said Washington State Patrol Trooper Kevin Fortino. The number of line cutting reports have seen a spike. In 2017, a total of 2,866 complaints came in. That's well above the 1,600 from 2016.

	And it could get worse now that it's near the peak season. “As we get into the summer months, that's kind of the Super Bowl for line cutting,” said Ian Sterling, spokesperson for the Washington State Ferries. Line cutting can bring a $136 fine, but whether that’s issued is up to the trooper’s discretion.
Return to Top	

HEADLINE	**04/27 Hit-run crashes rise locally**
SOURCE	**http://komonews.com/news/local/hit-and-run-crashes-on-the-rise-nationally-and-locally**
GIST	MARYSVILLE, Wash. - More than one hit and run crash happens every minute in the U.S. according to a new nationwide study from the AAA Foundation for Traffic Safety. The study said pedestrians and bicyclists are most at risk. Here in the Puget Sound region, we've seen those same staggering numbers. According to the Washington State Patrol, already this year, there have been more than 700 hit and run crashes in our state. •249 in King County •157 in Snohomish County •116 in Pierce and Thurston Counties Trooper said in 63 percent of those crashes, investigators have not been able to track down the responsible driver.
Return to Top	

HEADLINE	**04/26 FBI campaign: sex assault on planes**
SOURCE	**https://www.kiro7.com/news/local/fbi-launches-campaign-about-sexual-assault-on-aircraft/739308620**
GIST	SEATAC, Wash. - The FBI on Thursday launched a new campaign about sexual assault on aircraft, reminding passengers it is a federal crime and urging victims to come forward. Special Agent Bruce Reynolds said even, if an assault happened years ago, FBI agents want to hear from passengers. "I believe it's an underreported crime. A lot of times people are reluctant to come forward," Reynolds said. The FBI said the number of reports of sexual assaults on airplanes has risen from 38 in fiscal year 2014 to 63 in the fiscal year that ended in 2017. The FBI's new public message urges passengers to take precautions, such as booking children traveling alone in aisle seats so flight attendants can easily see if they're safe, keeping armrests down and asking to be reseated if your gut tells you someone's behavior is suspicious. Reynolds also suggests passengers "not be in a situation where you consume too much alcohol, or maybe on long flights, overnight flights, where you take sleeping pills." Delta Air Lines declined comment on Dvaladze's lawsuit but said in a statement that Delta crews are "trained to respond to a number of onboard passenger disruptions."

	Alaska Airlines also recently started new training for its crews. Sen. Patty Murray, D-Washington, sponsored a bill requiring that onboard sexual misconduct be reported to a law enforcement agency.
Return to Top	

HEADLINE	**04/26 Renton child luring suspect arrested**
SOURCE	**http://q13fox.com/2017/12/20/tips-help-renton-police-id-suspect-accused-of-groping-exposing-himself-to-young-girls/**
GIST	FUGITIVE CAPTURED IN VERMONT — April 25, 2018 After four months on the run, Border Patrol agents in Vermont spotted Remy Amon walking down a road on Wednesday. He was taken into custody and turned over to the Vermont State Patrol. The 41-year-old is being held on $500,000 bail in the Northwest State Correctional Facility in Swanton, Vermont. Amon will now face extradition back to Washington state. Official press release from U.S. Customs and Border Protection: *Alburgh, Vt. – U.S. Border Patrol agents apprehended Remy Amon, 41, an Ivory Coast national with an extraditable felony warrant for molestation of a child.* *At approximately 7:30 p.m. on Wednesday, Border Patrol agents in Alburgh, VT encountered Amon walking in the rain on Rt. 2 wearing a large coat and carrying a backpack. This area is in close proximity to the international border and agents routinely encounter subjects who have illegally entered the U.S. in this area.* *During questioning, the agent attempted to identify Amon, however, he stated his identification documents had been stolen. Agents transported him to the Swanton Station where biometric record checks revealed that he had initially provided a false name to agents and not only had no status or documentation to allow him to legally enter or be present in the United States, has an extensive criminal history including a warrant for arrest.* "This arrest is a great example of why the work of our Border Patrol agents along the northern border is so important," said Swanton Station Patrol Agent in Charge Matthew Sherman. "The agents' diligence in identifying this individual means we were able to remove a dangerous criminal from our community." Border Patrol contacted the King County Sheriff's Office in Washington State who will extradite Amon based on the warrant for molestation of a minor.
Return to Top	

HEADLINE	**04/26 State working thru rape kit backlog**
SOURCE	**http://q13fox.com/2018/04/26/washington-working-through-rape-kit-backlog-but-has-several-thousand-to-go/**
GIST	FEDERAL WAY, Wash. -- Authorities say DNA evidence led to the arrest of the so-called Golden State Killer this week, who is believed to have raped 51 women over several years. But what about DNA that is in the hands of investigators right now, just waiting to be processed? The state of Washington has a huge backlog of untested rape kits that hold evidence that could point to the attackers.

	It's something law enforcement is working to solve. Q13 News reporter Simone Del Rosario questioned Capt. Monica Alexander of Washington State Patrol about the process. Q: How did this backlog happen in the first place? A: People were not submitting kits once upon a time, if they didn't have a suspect, there were different reasons why kits were not submitted. And then when the law was passed that every kit had to be tested, that's when we realized there's a lot of kits out there and there's a lot more kits than there are people to process those kits. Q: What are we looking at backlog wise? How many kits do we think are out there? A: We're looking at anywhere between 7,000 and maybe as high as 10,000 kits now. Q: What's been the result of testing some of these kits? What have we found out? A: We've had 121 matches since they've been uploaded into CODIS and we've had 345 uploaded into CODIS. What that tells us is that's good information we can pass back to law enforcement agencies that submit those kits and now they can start trying to put that together with the case work that they're doing. Q: So what's going to take priority: Is it the new rape test kit that comes in or some of the backlog? A: You can state that there's a rush and we have to evaluate that on a case-by-case basis, so that's the responsibility of laboratory managers to prioritize those cases depending on what the law enforcement agency shares with us. Q: When would we be able to erase this backlog and address just the kits coming in? A: With what we have right now it would take probably two and a half to five years to clear out all the backlog. When you put the new cases on top of that, I really don't have an answer for that because we never know day by day how many cases we're going to get in. Q: For a victim, what does this do for peace of mind? A: When the police go out and arrest them and they're prosecuted for their crime, it changes people's lives. It absolutely changes these people's lives. And I think we keep that in our mind and it's frustrating when we have this DNA but we just don't have enough people to process it or a large enough lab to process it, but I believe very strongly with the way that technology is moving so quickly forward, this isn't going to be a problem for long.
Return to Top	

HEADLINE	**04/27 Bosnia detains 12; suspicion war crimes**
SOURCE	**http://www.foxnews.com/world/2018/04/27/senior-wartime-bosnian-officer-detained-for-war-crimes.html**
GIST	SARAJEVO, Bosnia-Herzegovina – Authorities in Bosnia say police have detained a former Bosnian army commander and 11 others on suspicion of war crimes against Serb and Bosnian civilians and prisoners during the 1992-95 war. The prosecutor's office says Atif Dudakovic and other commanders and members of the wartime Bosnian army's 5th Corps were detained in early-morning raids Friday in several towns. Dudakovic was in charge of the northwestern Bihac area which was under Serb siege during most of the conflict. The 64-year-old former general became the Bosnian army commander after the war.

	The prosecutor's office says Dudakovic and others are suspected of atrocities against hundreds of Serbs and Bosniaks. It says the case against the group is based on hundreds of testimonies, video footage and other evidence. The probe opened in 2005.
Return to Top	

HEADLINE	**04/26 Latin America amidst murder crisis**
SOURCE	**https://www.theguardian.com/world/2018/apr/26/latin-america-murder-crisis-violence-homicide-report**
GIST	Latin America has suffered more than 2.5m murders since the start of this century and is facing an acute public security crisis that demands urgent and innovative solutions, a new report warns. “The sheer dimensions of homicidal violence are breathtaking,” says the report by the Igarapé Institute, a Brazil-based thinktank focused on security and development issues. The publication, released on Thursday, paints a bleak portrait of what it calls the world’s most homicidal continent. Latin America suffers 33% of the world’s homicides despite having only 8% of its population. One-quarter of all global homicides are concentrated in four countries – Brazil, Colombia, Mexico and Venezuela – all of which are gearing up for presidential elections in which security is a dominant theme. “The overall trend right now in Latin America is one of increasing homicides and deteriorating security,” said Robert Muggah, one of the report’s authors. “Latin America is a large area and there are lots of variations. But as a region – including Mexico down to Central America and South America – the rate of homicide is set to continue increasing up until 2030. The only other places we are seeing similar kinds of increases are in parts of southern and central Africa and some war zones.” The report lays bare how young Latin Americans are disproportionately affected, with nearly half of all homicide victims aged 15–29. It also denounces the “astonishingly” large role of guns. Muggah said: “In addition to having these exceedingly high, epidemic levels of homicide, the vast majority of these homicides are committed with firearms. Over 75% of homicides are gun-related.” The global average is about 40%.
Return to Top	

HEADLINE	**04/26 Charges dropped: teen ‘planned’ shooting**
SOURCE	**https://www.cbsnews.com/news/charges-dropped-against-jack-sawyer-teen-accused-of-threatening-school-shooting-in-vermont/**
GIST	The thin line between planning a school massacre and attempting it has a teenage suspect on the verge of walking free in Vermont. Now, the community is on edge. At Fair Haven Union High School, attendance has been down as much as 25 percent in the last two months. "He threatened to kill a lot of people in our school," said one student at the school. Jack Sawyer, a former student, carefully detailed his plan to shoot up the school in a journal entitled "The

	journal of an active shooter." It listed who he wanted to kill, like the school resource officer, saying, "I'm intending to just blow his (expletive) head off before he can even draw his gun or think about what's happening.'" The plot was foiled when Angela McDevitt, a 17-year-old acquaintance of Sawyer's from upstate New York, was texting with him on the day of the Parkland, Florida, shooting. McDevitt thought a mutual friend of theirs might have been a student at Marjory Stoneman Douglas High School. "I went to Jack, and I was like ,'Hey, this girl who we both know, school just got shot up,'" she said. In response, she said he told her, "That's fantastic. I 100 percent support it. What school was it?" McDevitt told the police officer at her school, who quickly called the Vermont State Police. Prosecutors charged Sawyer with attempted murder and aggravated assault. But they weren't expecting a 112-year-old law to get in the way. In Vermont, "planning" isn't "attempting." So last week, hard as it may be to believe, prosecutors were forced to drop the felony charges against Sawyer, after the Supreme Court ruled there was "no attempt," since the act had not been committed. "When you look at it, telling the detectives you're just delaying by law enforcement interactions," said Bill Humphries, the Fair Haven police chief. "I understand their ruling, I don't agree with it, but I mean those are the kind of laws we have to live with right now." If Sawyer can make the reduced bail, he must seek mental health help, but he will get out of jail. That leaves principal Jason Rasco dealing with panicked students and anxious faculty. No school in America lives without fear these days, but the threat at Fair Haven Union High seems a little more real.
Return to Top	

HEADLINE	**04/26 Rape kit backlog blamed in assault**
SOURCE	**https://www.king5.com/article/news/local/rape-kit-backlog-blamed-in-second-assault-in-tumwater/281-546341443**
GIST	A sexual assault case in Tumwater provides a glaring example of how Washington state's rape kit backlog is still having serious and devastating consequences. Tumwater police have linked suspect Logan Humphrey, 35, to two violent sexual assaults that occurred within six months of each other, but it took police months to obtain DNA evidence that could have potentially put the suspect behind bars before the second crime occurred. Detectives first opened the case in July 2017 when a woman was threatened at knife-point and raped in a wooded area near Tyee Drive, according to the police report. Tumwater police Lt. Jen Kolb said, "it caused us great concern that he had the capability of doing it again." A sexual assault kit containing critical DNA evidence was taken immediately after the crime, but Tumwater police say they didn't receive the results until January 23, 2018, around six months later, finally allowing them to arrest the suspect on January 25. However, DNA evidence links that same suspect to another Tumwater sexual assault that occurred on January 22, the day before the first case's DNA results were relayed to police.

	"You hear something this horrific and it worries me how many sexual assault offenders have we left on the streets?" said Washington state Representative Tina Orwall, D-Des Moines, one of the lead lawmakers fighting to fix the state's rape kit backlog. While progress has been made since she began working on the issue several years ago, she says this case highlights the problem is far from being solved. "It's heart-wrenching to think somebody suffered when maybe we could have gotten this dangerous person off the streets so they couldn't have harmed anyone else, and I worry every day when I think about the 10,000 kits we haven't finished testing, or the new ones in the lab," said Orwall. "It speaks to needing to have urgency to have every kit tested." In a statement Thursday night, a spokesman with Washington State Patrol said the department believes it's vital to test every sexual assault kit sent to the state crime lab but noted that due to the large volume of DNA cases, scientists have to prioritize cases. The July rape in Tumwater was granted priority status, according to WSP. Lab techs required additional evidence to process the case resulting in it being assigned to a scientist a month later on August 30, 2017, according to a spokesman. However, it still took several months to complete the case and receive a "Combined DNA Index System" or CODIS hit. WSP confirms the forensic scientist on the case called Tumwater PD on January 23; a final report was issued January 30. "There are a multitude of factors which play a role in the amount of time it takes to complete a DNA case. These factors include the complexity of the case, whether or not the DNA has a CODIS hit and the technical review required of each case," said spokesman Kyle Moore. In addition to sexual assault cases, the State Crime Lab also processes homicides and other violent crimes. In 2017, the median DNA case took around 198 days, or more than six months to complete, according to Moore.
Return to Top	

HEADLINE	**04/26 DNA from genealogy site aided capture**
SOURCE	**http://abcnews.go.com/US/wireStory/accused-serial-rapist-killer-undetected-working-cop-54741076?cid=clicksource_81_2_hero_headlines_headlines_hed**
GIST	More than three decades after his trail went cold, one of California's most prolific and elusive serial killers was caught when investigators matched crime-scene DNA with genetic material stored by a relative on an online genealogical site, prosecutors said Thursday. Authorities have said the DNA tied former police officer Joseph James DeAngelo, 72, to most of the 12 killings he is accused of committing between 1976 and 1986 as part of the Golden State Killer case. Investigators also allege DeAngelo raped more than 50 women during that period. Authorities declined to name the DNA site used to track the DNA. Companies such as Ancestry.com and 23andMe charge customers to use their DNA to produce genetic profiles that determine ethnicity and can identify long-lost relatives, among other services. Both companies said Thursday they weren't involved in the case against DeAngelo. Sacramento County District Attorney Anne Marie Schubert said investigators surreptitiously obtained his DNA last week from discarded material that ended up matching DNA at crime scenes. Police received thousands of tips over the years, but DeAngelo's name had not been on the radar of law enforcement before last week, Schubert said.

	In other developments Thursday, police in Visalia said DeAngelo is a suspect in the 1975 killing of community college teacher Claude Snelling in the farming community about 40 miles (64 kilometers) south of Fresno. If the link is confirmed, it would boost the number of victims to 13 in the serial killing case. DeAngelo worked as a police officer in nearby Exeter from 1973 to 1976, and police in the region believe he also is the Visalia Ransacker, responsible for the death of Snelling, who was fatally shot while stopping someone from kidnapping his 16-year-old daughter, and about 100 burglaries. Visalia police Chief Jason Salazar said Snelling's death and the region's burglaries weren't part of the tally of crimes authorities released Wednesday in the serial killing case because investigators lacked DNA evidence on those crimes. Salazar said fingerprints and shoe tracks will be eyed for matches to DeAngelo. Detectives are also looking to see if any items taken during the Visalia burglaries are uncovered during the investigation. In addition, DeAngelo matches the description of Snelling's killer, Salazar said, and the attacker used sophisticated pry tools to gain entrance to locked homes, just as authorities say DeAngelo did in other crimes. The culprit also wore a ski mask and eluded capture because of an apparent deep-knowledge of police work. "He always had a good escape route," Salazar said.
Return to Top	

HEADLINE	**04/27 Pakistan first conviction for child porn**
SOURCE	**http://abcnews.go.com/International/wireStory/pakistan-sentences-man-conviction-child-porn-54773855?**
GIST	A Pakistani court in the eastern city of Sargodha has sentenced a man to seven years in prison for working for a child pornography network, the first such conviction in this Islamic nation. District police chief Suhail Chaudhry says the court's ruling against Sadat Amin was announced on Thursday. He says Amin was arrested earlier this month by the Federal Investigation Agency — Pakistan's version of the FBI — following a complaint from the Norwegian government. The police chief says the investigation proved Amin produced and sold porn videos of children to a Norway-based network. During the trial, prosecutors said Amin confessed to luring children to produce porn videos. Pakistan recently introduced laws giving authorities power to crack down on the porn industry.
Return to Top	

HEADLINE	**04/26 Suspected serial killer 'shocked by arrest'**
SOURCE	**http://abcnews.go.com/US/suspected-golden-state-killer-shocked-arrest-told-police/story?id=54746113**
GIST	The suspected "Golden State Killer" who was arrested this week for killing and raping dozens of California residents decades ago, seemed shocked to find police outside his home, according to Sacramento County Sheriff's Department official Paul Belli.

	Joseph James DeAngelo, a 72-year-old former police officer, was taken into custody on Tuesday at his home in Citrus Heights in Sacramento County, the same county where his alleged crime spree began in 1976. The crimes continued across the state until 1986. DeAngelo lived at the home with family but was home alone when he was arrested, Belli told ABC News. DeAngelo told police he had a roast in the oven, and officers said they could take care of it, Belli said. He was placed under arrest without incident. DeAngelo is believed to have committed 12 murders, at least 50 rapes and multiple home burglaries in the 1970s and 1980s. His alleged "reign of terror" spanned from the Sacramento area in Northern California down to Orange County in Southern California, Orange County District Attorney Tony Rackauckas said Wednesday. DeAngelo served in the Navy in the 1960s. An Auburn Journal article from 1967 said DeAngelo was a sailor aboard the USS Canberra. DeAngelo was a police officer in Exeter, California, from 1973 to 1976, officials said. In 1976 he served as a police officer in the city of Auburn until he was fired in 1979 for allegedly stealing a hammer and a can of dog repellent, The Associated Press reported, citing Auburn Journal articles from the time. DeAngelo then spent 27 years working for Save Mart Supermarkets at a distribution center in Roseville, near Sacramento, said Victoria Castro, a public affairs manager for Save Mart. He retired last year. "None of his actions in the workplace would have lead us to suspect any connection to crimes being attributed to him," Castro said in a statement. "We are working with the Sacramento County District Attorney's Office on their investigation."
Return to Top	

HEADLINE	**04/26 Bill Cosby found guilty on all charges**
SOURCE	**http://abcnews.go.com/US/bill-cosby-found-guilty-charges/story?id=54746891&cid=clicksource_81_2_hero_headlines_headlines_hed**
GIST	It was a long, uphill battle, years in the making, but prosecutors in Montgomery County, Pennsylvania, finally won the conviction on felony sexual assault charges of the man once revered as “America’s Dad.” At the age of 80, Bill Cosby was convicted today on three felony counts of aggravated indecent assault stemming from drugging and molesting a woman in his suburban Philadelphia home 14 years ago. As the verdict was read just before 2 p.m. in the Montgomery County Courthouse in Norristown, Pennsylvania, Cosby leaned his head down, took a deep breath and appeared to close his eyes. Cosby's main accuser, Andrea Constand, and two other women who say Cosby also drugged and sexually assaulted them were in the courtroom and burst into tears as the verdict was announced. "I feel like my faith in humanity has been restored," one of the women, Lili Bernard, said after hearing the verdict. "I stand here in the spirit of Martin Luther King, who said that the arc of the moral universe is long but today it has bent towards justice. "Today, this jury has shown what the #MeTo movement is saying, that women are worthy of being

	believed," she said. "And I thank the jury, I thank the prosecution." The conviction came about 11 months after a mistrial was declared in Cosby's first trial when a jury failed to reach a verdict. The jury of seven men and five women began deliberating Wednesday and spent a little over 12 hours going over evidence presented to them over the last two weeks before rendering their unanimous decision. Judge O'Neill ordered Cosby to surrender his passport but ruled he can remain free on $1 million bail until his sentencing sometime in the next 60 to 90 days. He faces up to 30 years in prison.
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