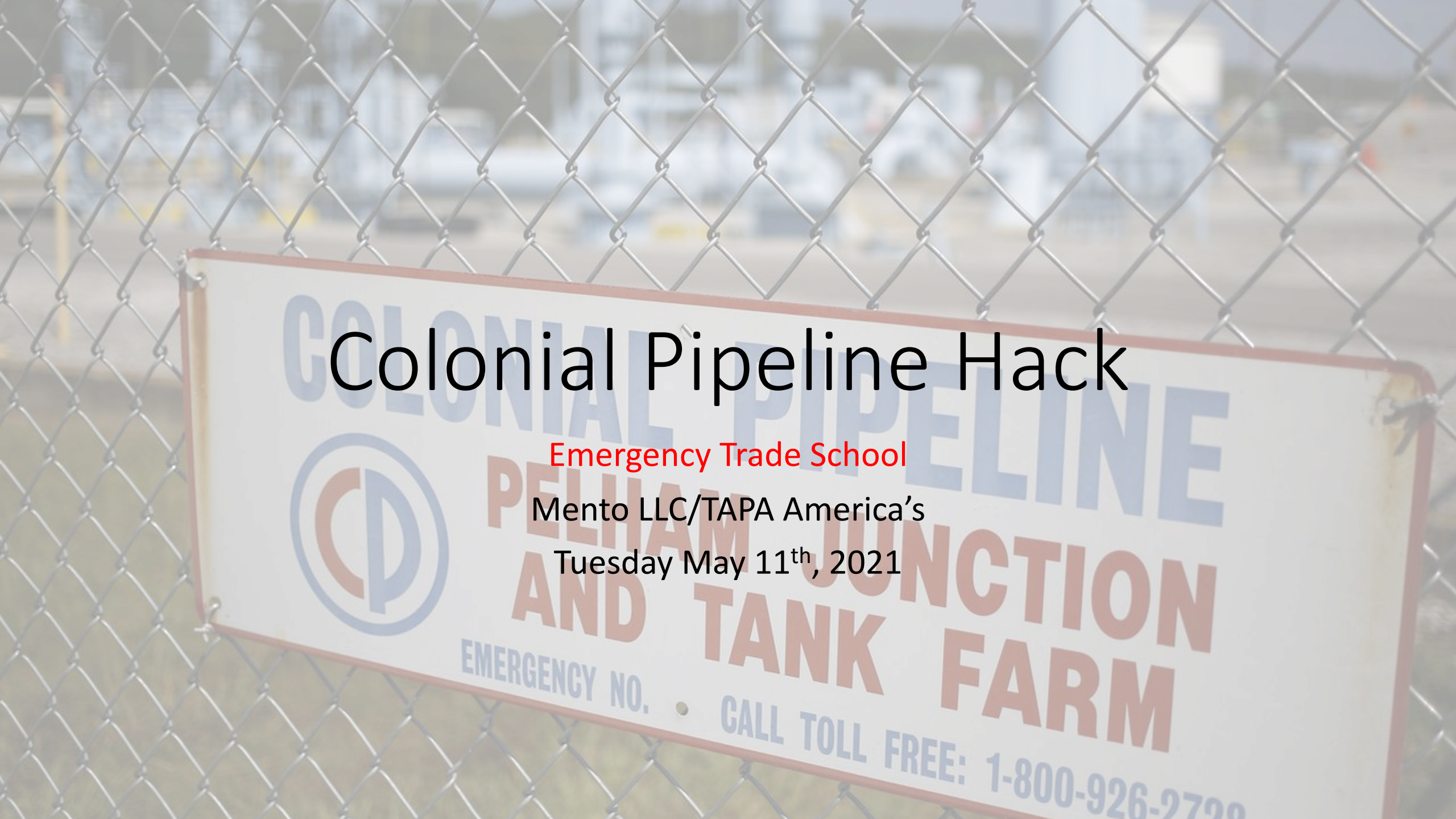


Colonial Pipeline Hack

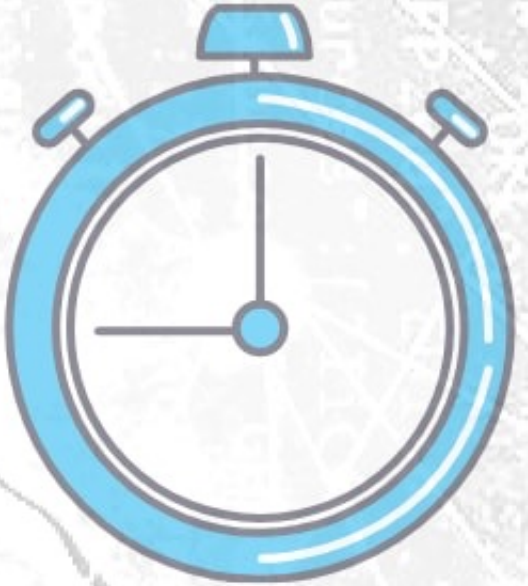
Emergency Trade School

Mento LLC/TAPA America's

Tuesday May 11th, 2021

Global Cybercrime Damage Costs:

- **$6 Trillion USD a Year. ***
- **$500 Billion a Month.**
- **$115.4 Billion a Week.**
- **$16.4 Billion a Day.**
- **$684.9 Million an Hour.**
- **$11.4 Million a Minute.**
- **$190,000 a Second.**



ALL FIGURES ARE PREDICTED BY 2021

* SOURCE: CYBERSECURITY VENTURES

CYBERSECURITY VENTURES

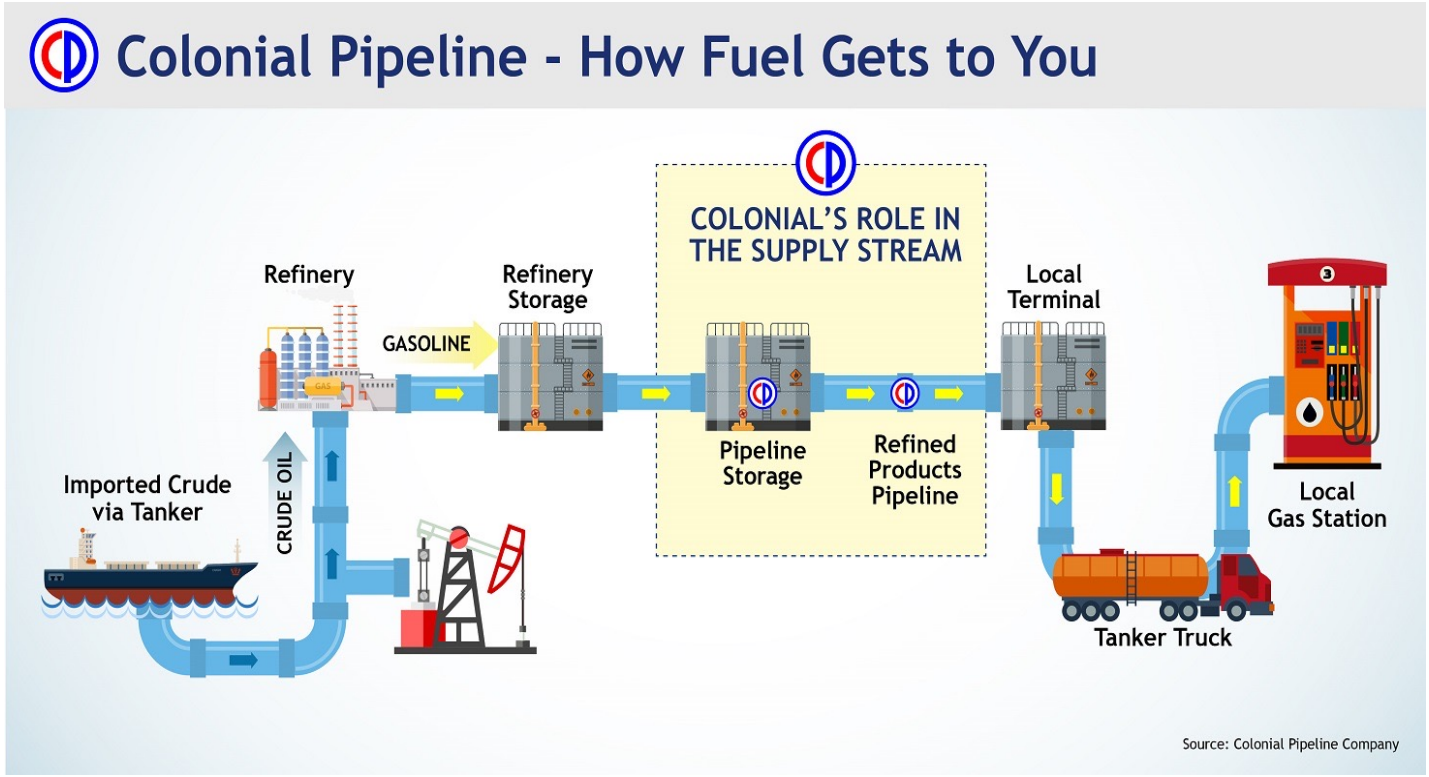
The Hack and the Pipeline

- The Colonial Pipeline, which delivers about 45% of the fuel used along the Eastern Seaboard, shut down Friday after a ransomware attack by gang of criminal hackers that calls itself DarkSide.

- Depending on how long the shutdown lasts, the incident could impact millions of consumers.

- Hackers broke into networks devoted to the company's business operations, it did not reach computers that control the physical infrastructure that transports gasoline and other fuel.

The Pipeline Conceptionally



- Colonial's network supplies fuel from U.S refiners on the Gulf Coast to the populous eastern and southern United States.

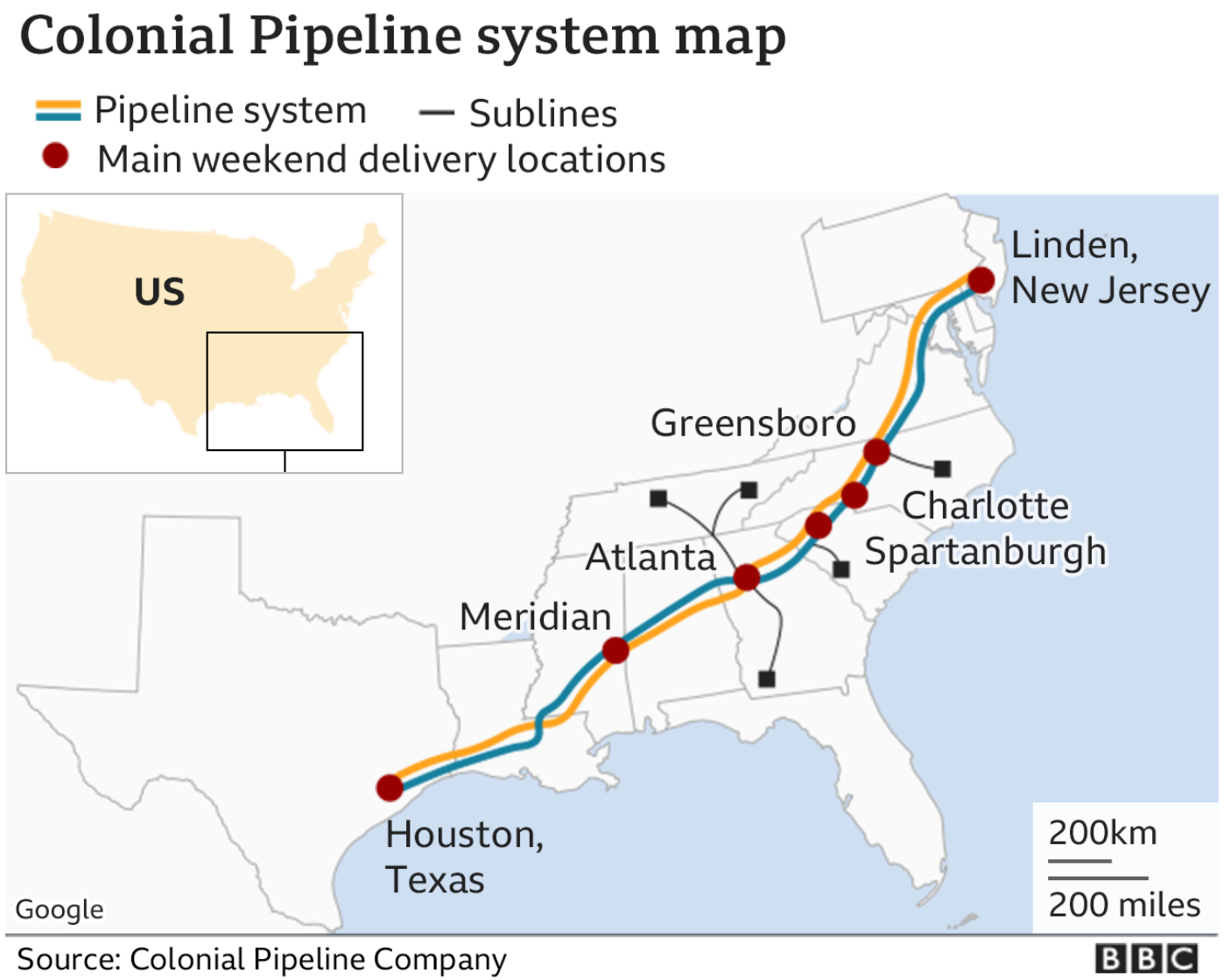
- The company transports 2.5 million barrels per day of gasoline, diesel, jet fuel and other refined products through 5,500 miles (8,850 km) of pipelines, and transports 45% of East Coast fuel supply.

COLONIAL PIPELINE MAP

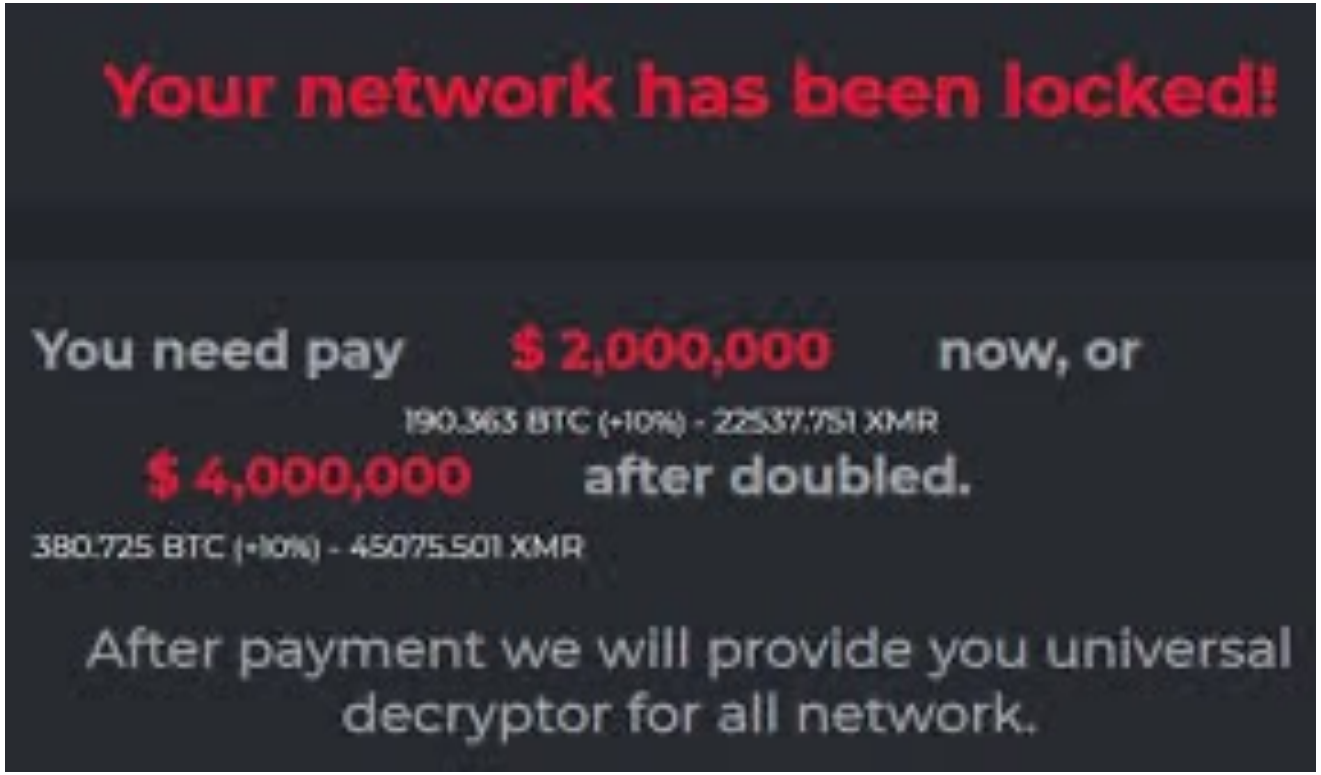
Source: Colonial

Disruptions – Of Course

- Both gasoline and diesel futures on the New York Mercantile Exchange rose more than crude prices during the day.
- Gasoline futures gained 0.6% to settle at $2.1269 a gallon, while diesel futures rose 1.1% to settle at $2.0106 a gallon.
- The fact that this attack compromised systems that control pipeline infrastructure indicates that either the attack was extremely sophisticated, or the systems were not well secured



Ransomeware



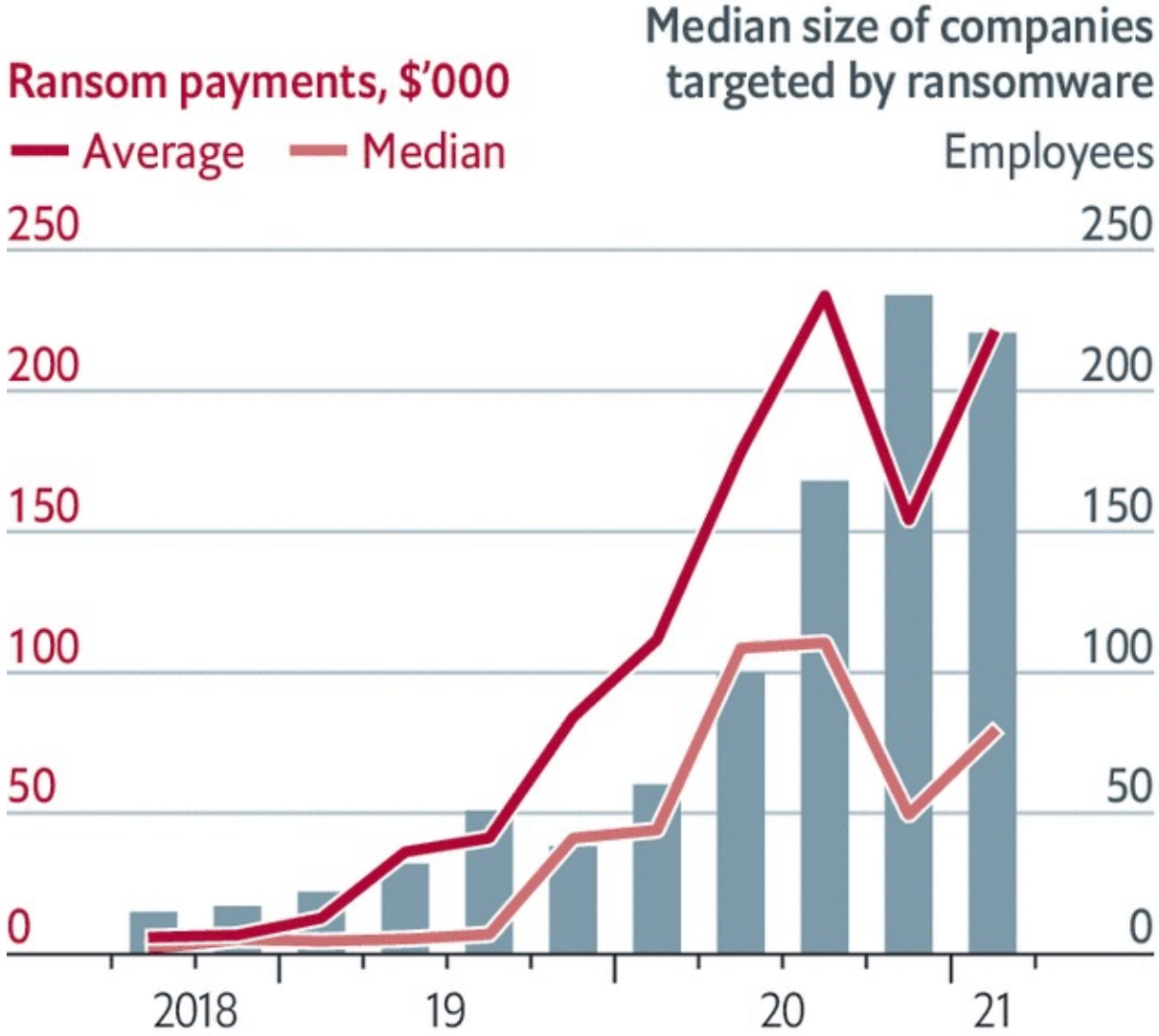
- Ransomware is a type of malware that is designed to lock down systems by encrypting data and demanding payment to regain access.

- The company shut down systems to contain the threat after learning of the attack on Friday, Colonial said in the statement.

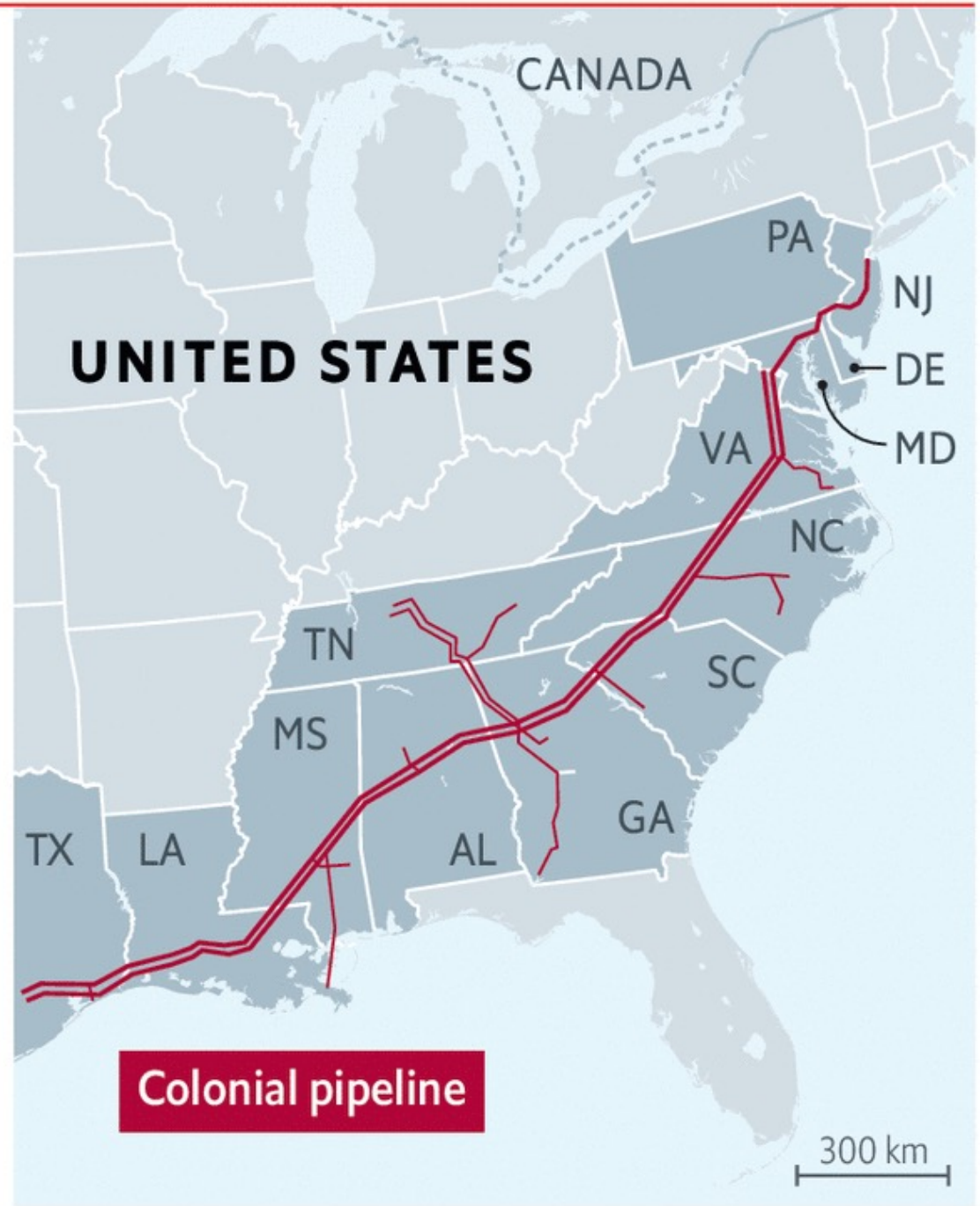
- That action has temporarily halted operations and affected some of its IT systems, the company said.

Striking oil

United States



Sources: Coveware; Colonial Pipeline Company



The Economist

DarkSide

- **“WE CREATED DARKSIDE** because we didn’t find the perfect product for us,” reads the launch announcement. “Now we have it.”

That’s a line that could come from my technology company. But it isn’t.

It’s the latest strain of ransomware built by Darkside to extort the largest of targets for millions, with attacks that are couched in an uncanny air of professionalism.

DarkSide

- Guaranteed turnaround times. Real-time chat support. Brand awareness.

- As ransomware becomes big business, its purveyors have embraced the tropes of legitimate enterprises, down to corporate responsibility pledges.

- In that same “press release,” posted to the operators' site on the dark web (8/10/2021) the DarkSide hackers “pinky-swear” not to attack hospitals, schools, nonprofits, or government targets.

DarkSide

When Ragnar Locker ransomware hackers struck the travel company CWT, a chipper representative at the other end of the support line broke down what services the ransom payment would render, offered a 20 percent discount for timely payment, and kept the chat window functional after handing over the decryption keys in case CWT needed any troubleshooting.

"It's a pleasure to deal with professionals," wrote the Ragnar agent as the conversation wound down. They might as well have been discussing a return of a package to Amazon ……

What we know about them -

- Very little really.
- Eastern European, likely Russian.
- Selling software to cybercriminals, they are more like a solutions provider than a cartel.
- They work almost exclusively in crypto currency and through the dark web.
- Nobody knows for sure how much their software has pinched, but the numbers are easily in the hundreds of Millions.

US Response to DarkSide

- Probably not much.
- DarkSide software is written to not work against businesses within Russia and Eastern Europe ….. Really?
- The US has known about this for years. Why hasn't action been taken before now? Because this has been seen as a situation best taken care of by industry.
- In short, it may be too big for governmental impact.
- Imagine that.

Rise of Organized Cybercrime

- The average cost of cybercrime for an organization has increased $1.4 million over the past year, to $13.0 million, and the average number of security breaches in the last year rose by 11 percent from 130 to 145.

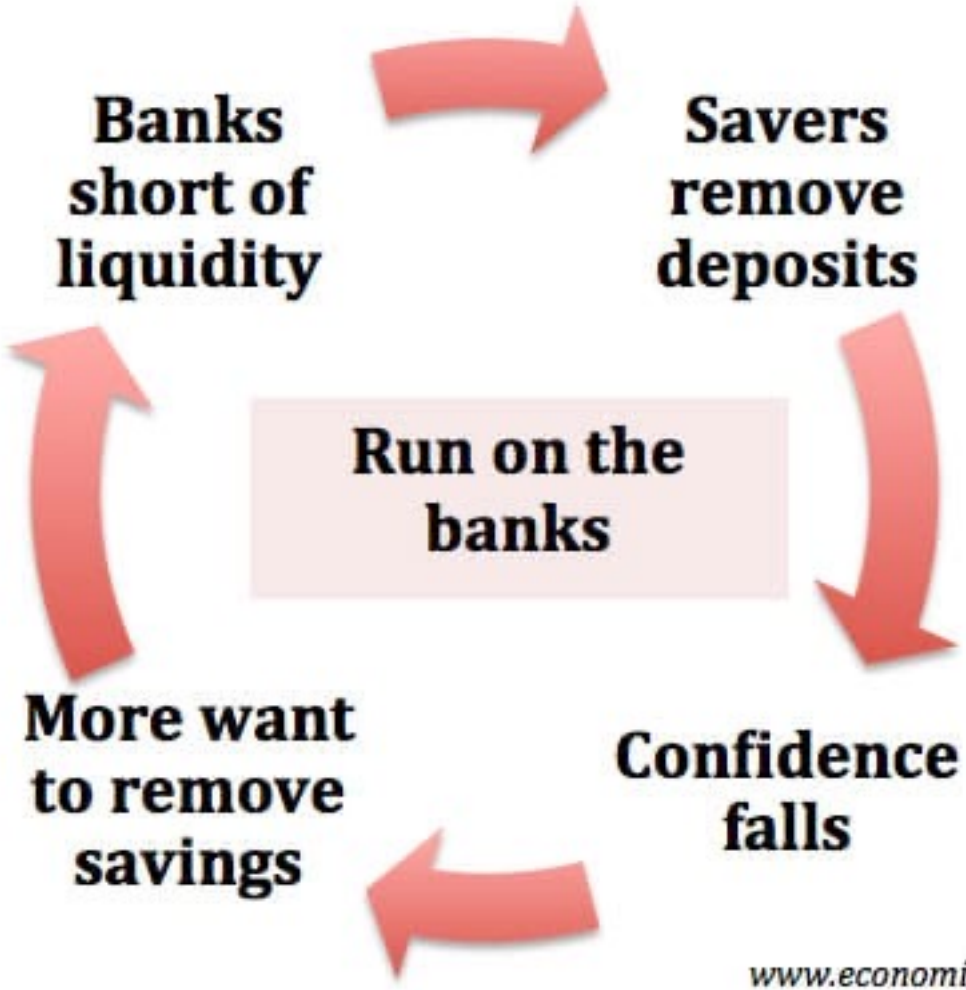
- An interesting development is when nation-states and their associated attack groups use these types of techniques to go after commercial businesses. Attempts are now being made to categorize attacks from these sources as "acts of war" to limit cyber security insurance settlements.

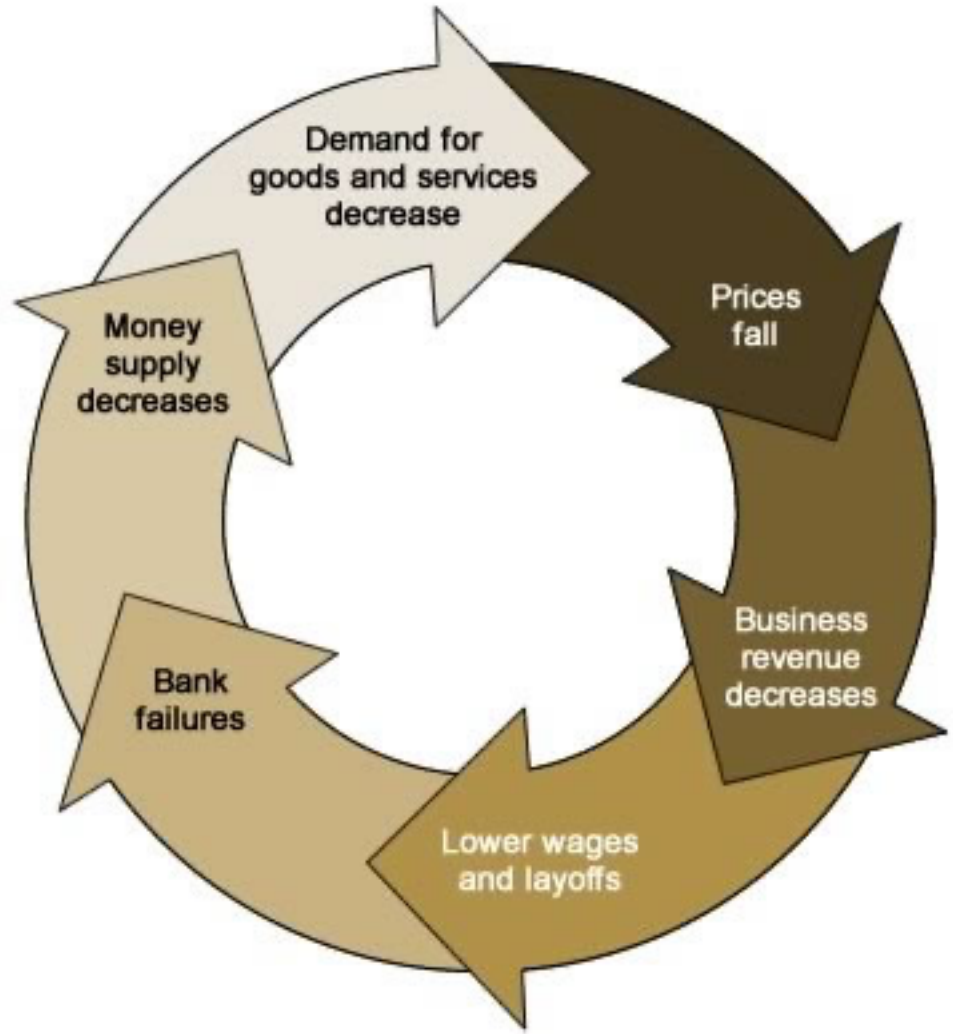
Rise of Organized Cybercrime

- Cyberattacks are the biggest risk for the country
- While the threat of a conventional attack is present, it become sless and likely as trade becomes ubiquitous.
- There is a degree of luck involved in pulling off a terrorist and surviving. With a cyberattack, one awful person and a laptop can bring down a country's critical infrastructure.
- And someone just did. Supposedly by accident.

Infrastructure/Confidence Attacks

- Pipelines
- Electric Grids
- Banks
- Internet
- Mobile Phone Networks
- Air Traffic Control
- Ports


Banks short of liquidity
Savers remove deposits
Run on the banks
Confidence falls
More want to remove savings
www.economicshelp.org


Demand for goods and services decrease
Prices fall
Business revenue decreases
Lower wages and layoffs
Bank failures
Money supply decreases

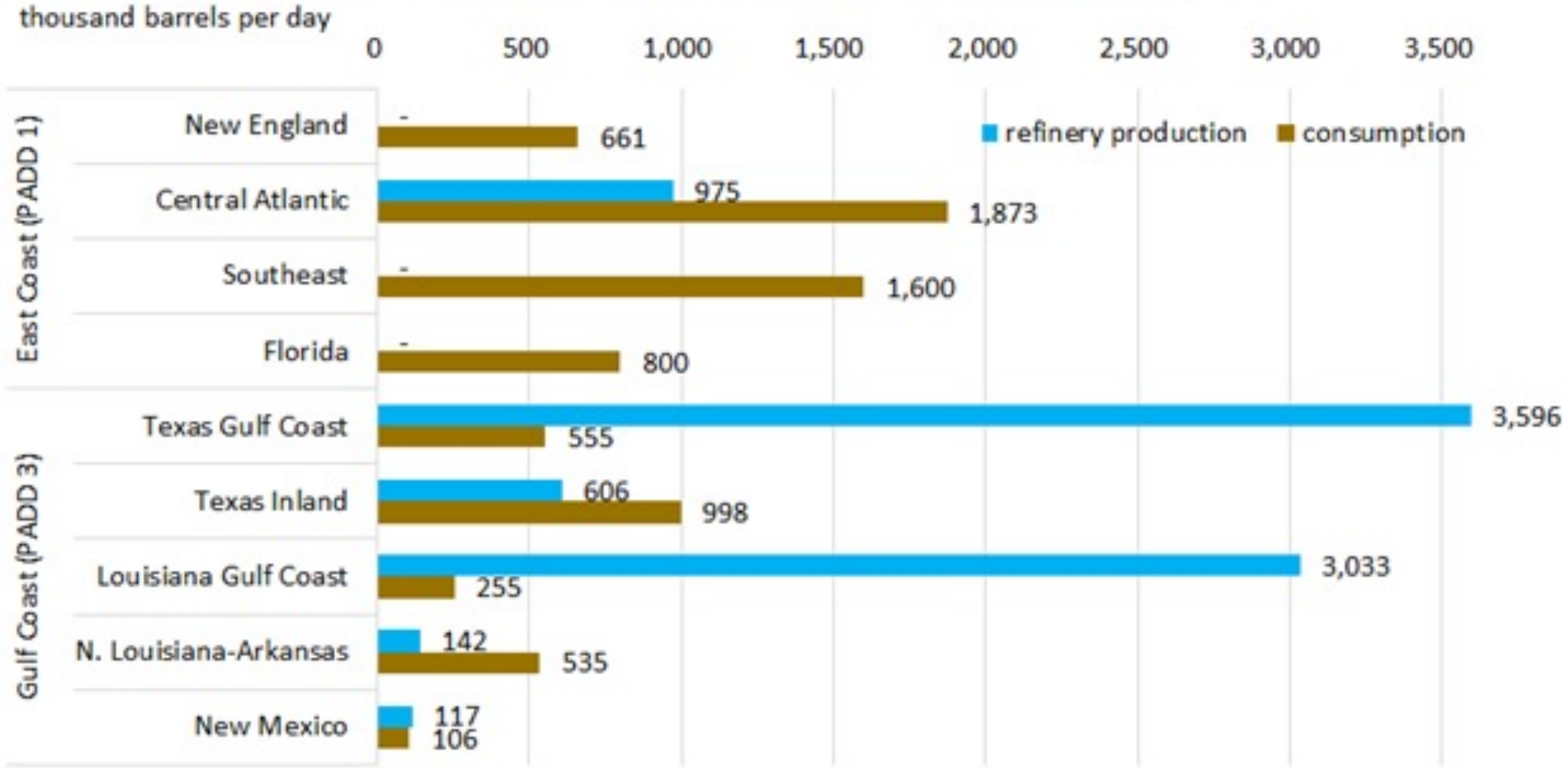
The Ugly Truth

- That is not the case for terrorists – a group can take down a power grid and there is nothing commensurate that the U.S. can target in response.

- That makes fighting cyberterrorism particularly challenging.

- And even easier for a nation state to distance themselves away from.

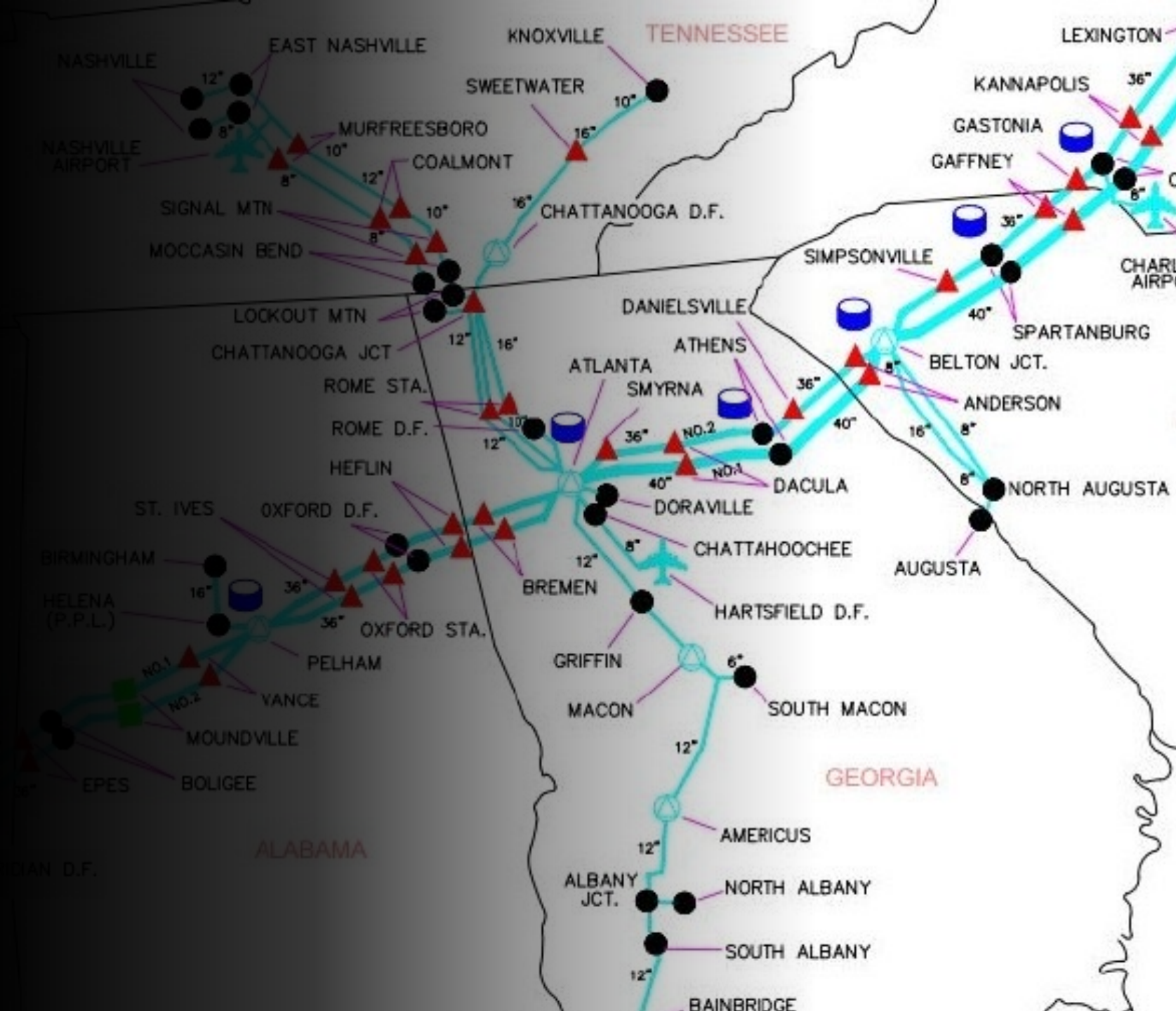
Figure 2. 2014 Regional transportation fuels production/consumption balance



Emergency Order

Emergency order lifts regulations on drivers carrying fuel in 17 states across the South and eastern United States, as well as the District of Columbia, allowing them to drive between fuel distributors and local gas stations on more overtime hours and less sleep than federal restrictions normally allow.

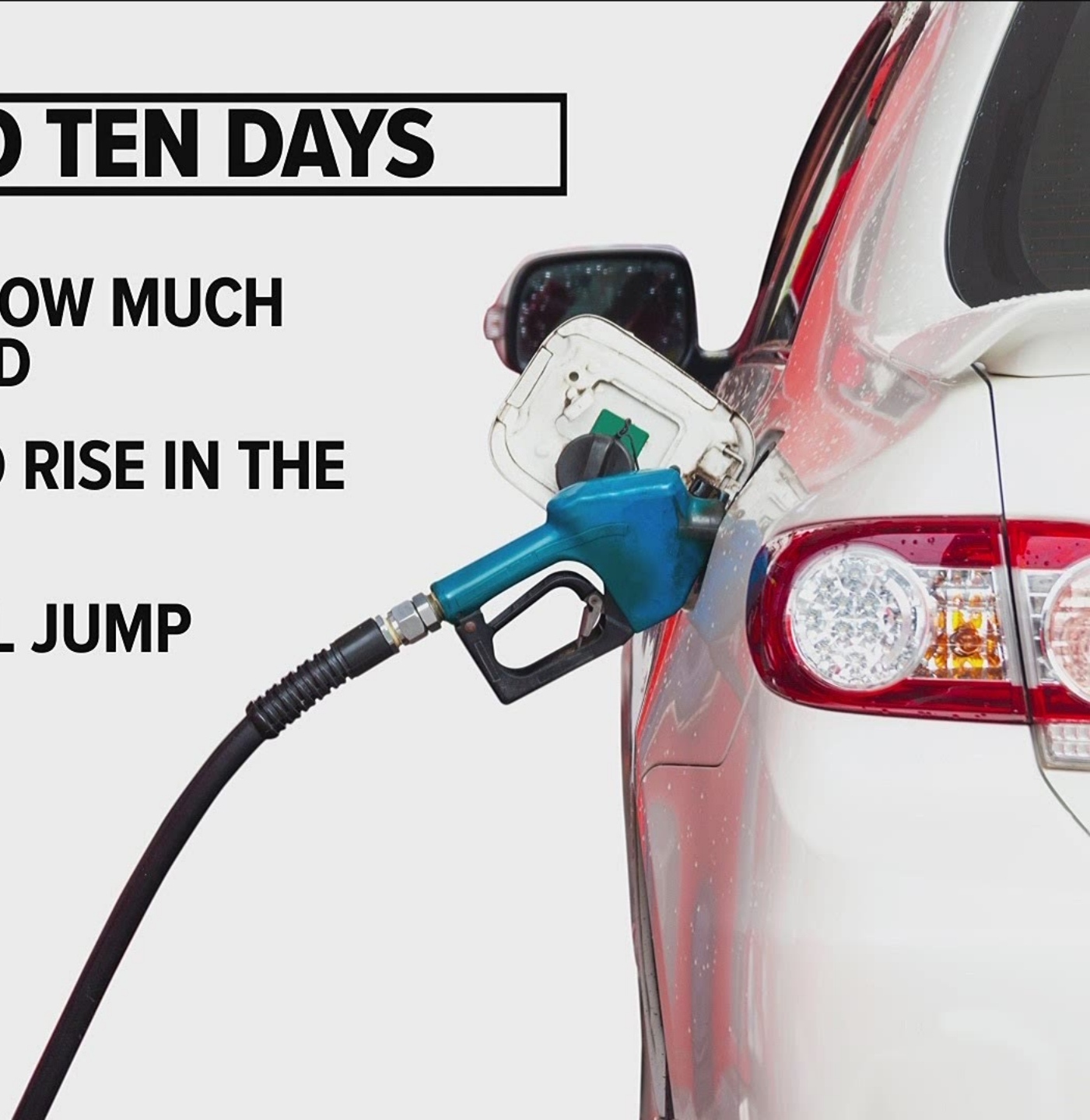
The U.S. is already dealing with a shortage of tanker truck drivers.



PIYAPHUNJUN - STOCK.ADOBE.COM

SIX TO TEN DAYS

- MAY NEED TO REDUCE HOW MUCH CRUDE OIL IS PROCESSED
- EXPECT INVENTORIES TO RISE IN THE GULF COAST
- PRICES IN THE EAST WILL JUMP
- SOME SHORTAGES



WILL GASOLINE PRICES GO UP?

- The average gas prices have jumped to $2.99 a gallon over the past week, and it's expected to continue climbing because of the pipeline closure, according to AAA.

- Mississippi, Tennessee and the East Coast from Georgia to Delaware are the most likely to experience limited fuel availability and higher prices, and if the national average rises by three more cents, these would be the highest prices since November 2014.

WILL THERE BE GASOLINE SHORTAGES?

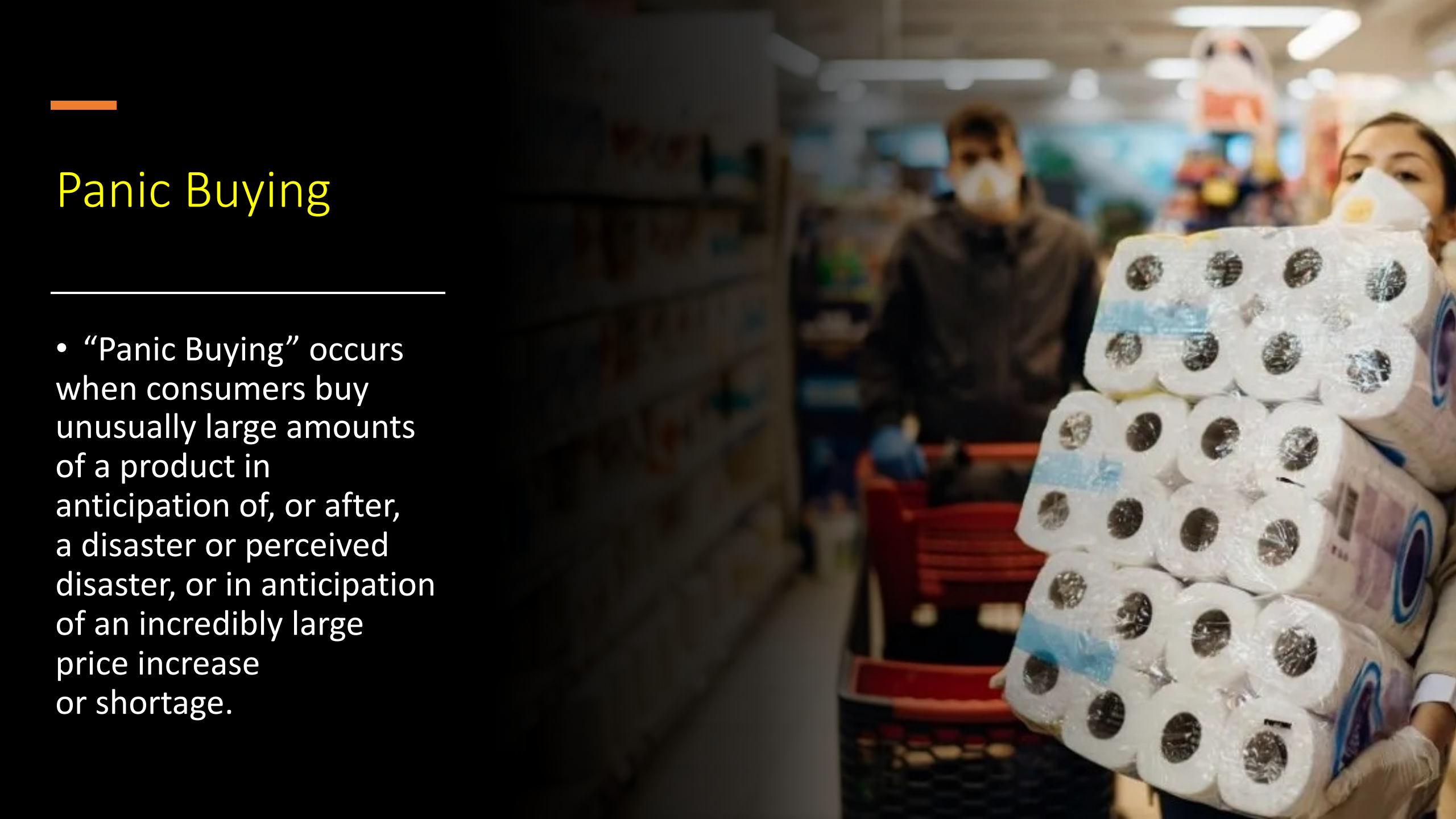
- It depends on how long the shutdown lasts. Colonial said it's likely to restore service on most of its pipeline by Friday.

- There’s no imminent shortfall, and thus no need to panic buy gasoline. If the pipeline is restored by Friday, there won’t be much of an issue.

- However, some gas stations along the East Coast have already begun running out of fuel. A few gas stations in Virginia and North Carolina have reported selling out of fuel

Panic Buying

- “Panic Buying” occurs when consumers buy unusually large amounts of a product in anticipation of, or after, a disaster or perceived disaster, or in anticipation of an incredibly large price increase or shortage.




Velvet
Velvet
Velvet
Velvet


WITHOUT RATIONING
RATIONING MEANS A FAIR SHARE FOR ALL OF US
RATION BOOK
RATION BOOK
WITH RATIONING
Office of Price Administration
Washington, D. C.


Select Product
Dispense Fuel
OUT OF GAS CURRENTLY
PUSH TO
RING
ATTENDANT
REGULAR
PLUS
PREMIUM
89
93


FREE

So we are going to fix all this right? Right?

- The President unveiled a $2 Trillion infrastructure plan that includes $100 billion to modernize the electrical grid.
- It provides $0 for cybersecurity infrastructure for this grid.
- President Biden also suspended the Trump bulk power system executive order so that he could introduce his own.
- He plans to unveil an executive order soon that will strengthen cybersecurity at federal agencies and for federal contractors.
- This does nothing to address private companies like Colonial.

So we are going to fix all this right? Right?

- The industry currently shares threats through NERC's Electricity Information Sharing and Analysis Center.

- But some members of the electric industry have voiced concerns the federal government does not provide enough guidance on critical vulnerabilities.

- The biggest change between Biden and Trumps plan is allowing for the use of foreign made components into critical energy infrastructure.

So we are going to fix all this right? Right?

- These measures are more focused on preventing another SolarWinds-like attack. Not like what we just saw.

- Keep in mind – this attack wasn't even that sophisticated.

- The oil pipeline attack might strengthen demands for cybersecurity standards for companies that play an important role in Americans' lives. As it stands, it's often left up to them about the security measures they use to protect critical systems.

CALL ME!!!!

978.317.3250
Pete.Mento@MentoLLC.com

Mento LLC