The Cyberattack: Colonial Pipeline

May - 2021

The Al-Attiyah Foundation

The Al-Attiyah Foundation is proudly supported by:

EXECUTIVE SUMMARY

What are the events, effects and implications of the Colonial Pipeline cyberattack in the United States?

- The Colonial Pipeline, the largest refined oil products system in the US, supplying 45% of east coast fuel, was shut down between 7-12th May by a cyberattack for ransom.
- Operations are now being restored, but there has been a brief spike in gasoline prices, and petrol stations in many east coast states have run out of fuel.
- While cyberattacks on the energy industry have become increasingly common, this recent attack on the Colonial Pipeline is the most high-profile incident in the US, to date.
- These cyberattacks may be for criminal (profit), espionage or sabotage (politically-motivated reasons), which can be related to various international disputes involving the US, Russia, Iran and other countries.
- The energy industry needs urgent steps and better security measures to limit its vulnerability to cyberattacks.
- However, no security can defeat a sufficiently capable and well-resourced attacker. Therefore, the energy system should, in general be made more resilient, in order to help protect against cyberattacks and other threats.

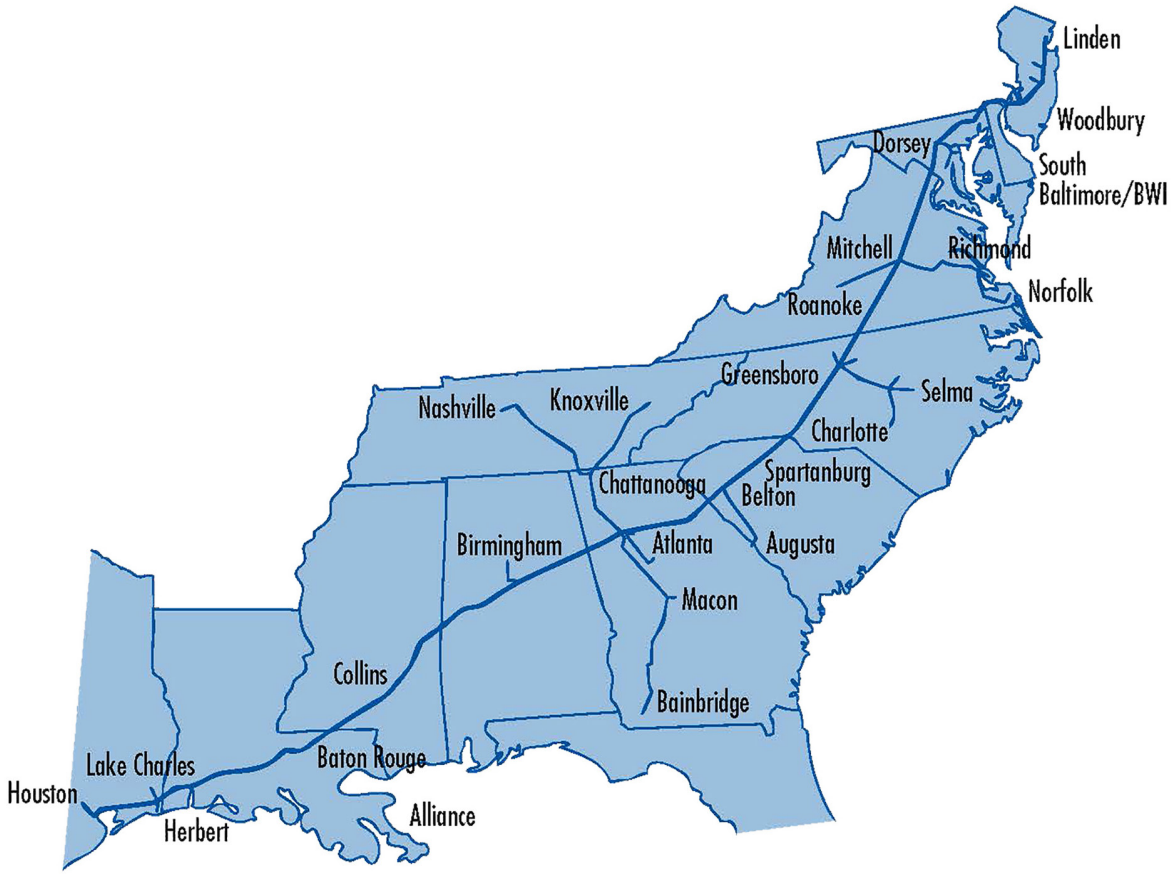
THE COLONIAL PIPELINE SYSTEM

The Colonial Pipeline is the key refined products pipeline in the eastern United States. It transports gasoline (petrol), diesel and jet fuel from the major refining centres on the Gulf of Mexico coast, in Texas and Louisiana to markets along the east coast, including the states of Alabama, Georgia, Tennessee, South Carolina, North Carolina, Virginia, Maryland and New Jersey.

The pipeline also connects to major onward lines in the north-eastern US, to New York and Pennsylvania.

The Colonial pipeline operates in batches to be able to ship different products, with a minimum size of 75 kbbl for Lines 1 and 2 and 25 kbbl for Lines 3 and 4. Batches are scheduled in 5-day cycles and vary seasonally and according to demand.

Figure 1 Colonial Pipeline route[ii]



Colonial is a private company owned by six investors: Koch Industries (28.09%), South Korea National Pension Service and KKR via Keats Pipeline Investors (23.44%), Caisse de depot et placement de Quebec (16.55%), Shell Pipeline, a unit of the oil major (16.12%) and Industry Funds Management, an Australian investor (15.8%).

It is the largest refined products pipeline in the US, supplying about 45% of east coast demand. The pipeline is particularly important because of the Jones Act, that requires cargoes between US ports to be carried on American-built, crewed and flagged ships. This makes cabotage (intra-national) shipping expensive and limits capacity.

Table 1 Colonial Pipeline main components[i]

Line	Size (inch)	Route	Fuel	Capacity, Mbbl/day
Line 1	40	Houston-Greensboro, North Carolina	Gasoline	1.5
Line 2	36	Houston-Greensboro, North Carolina	Diesel, heating oil, jet fuel	1.2
Line 3		Greenboro-Linden, New Jersey	All	0.885
Line 4	32	Greensboro-Baltimore	All	0.7
Spurs		Atlanta-south Georgia; Atlanta-Tennessee; Greensboro-Raleigh-Durham, North Carolina; Mitchell, central Virginia-Richmond, Norfolk, Roanoke	Various	

EVENTS OF THE ATTACK

On Friday 7th May, the Colonial Pipeline found it had been hit by ransomware, which encrypts or locks systems until a ransom is paid. The company had to take some systems offline to avoid further damage, and this required it to halt operations. Although it appears its routine corporate IT system, not its operations system, was compromised, the company had to take the pre-emptive measure to avoid possible escalation of further attacks.

The attack was confirmed to be by DarkSide, a hacker-for-hire, which stole 100 gigabytes of Colonial's data before locking its systems[iii]. The group, believed to be based in Russia or Eastern Europe, issued a statement apologising for the disruption, saying it was apolitical and blaming its client. DarkSide's ransoms are typically in the single-digit million dollars.

Colonial's operations are quite complex because of its multiple lines, fuel types and qualities, and number of shippers and the elaborate procedures for capacity nomination. This makes returning to service much more difficult than it would be for a simple crude oil pipeline.

The US government and state governors took various measures to ease the problem, including declaring a state of emergency, waiving fuel quality specifications, and lifting weight and driving hours restrictions for tanker trucks. The Department of Homeland Security was ready to consider requests for waivers of the Jones Act to permit maritime shipments from other US ports.

By 11th May, Colonial had returned Line 4 to service under manual control, using existing inventories[iv] . On 12th May, the company announced it would restart operations, but that it could take several days to return to normal.

IMPACT

Gasoline shortages began noticeable by 10th May, with Virginia and North Carolina the worst hit initially (Figure 2). By late on 12th May, Georgia, North Carolina, South Carolina and Virginia were greatly affected, with between half and two-thirds of stations out of gasoline. Several other states, such as Tennessee, began to see serious effects the same day. The shortages were driven by three factors:

- The lack of fuel driven by the pipeline outage itself;
- A lack of diesel, which prevented fuel trucks from making deliveries to stations;
- Panic-buying by motorists who feared running out of fuel.

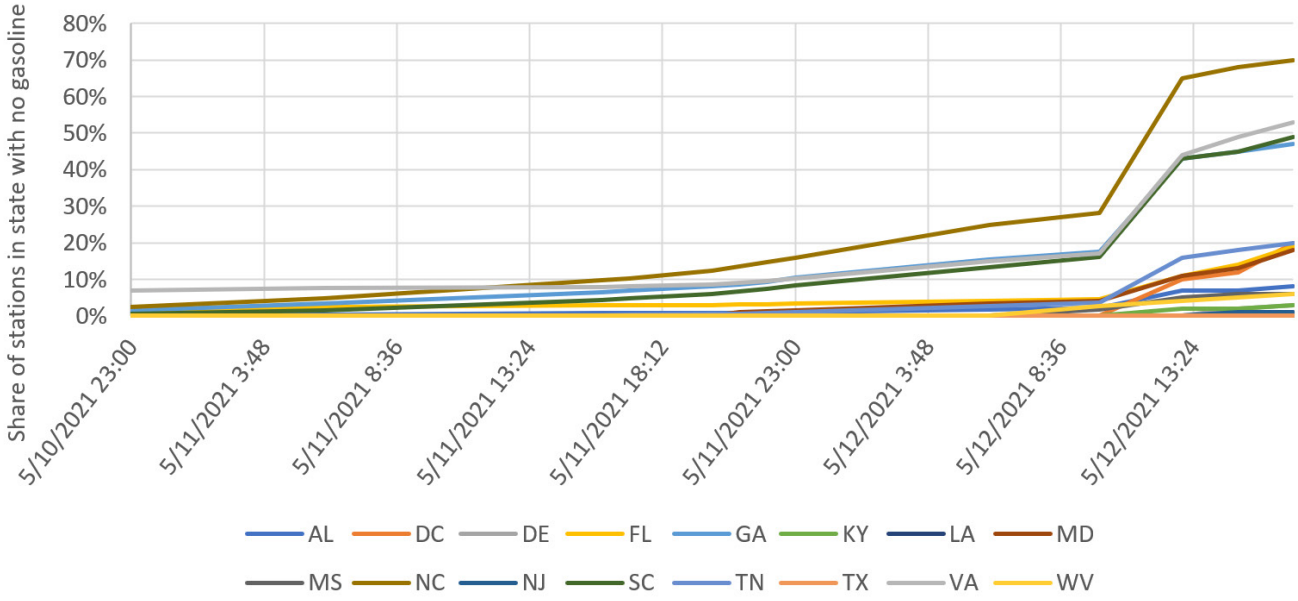
For instance, Florida, which is mainly supplied by barge from the Gulf Coast, also experienced some shortages, probably due to panic buying. The inland states, such as Tennessee, are likely to be worst-affected as the problem proceeds, as they do not have access to seaborne deliveries.

The lack of offtake capacity would also force Gulf Coast refiners to reduce runs, if they exhaust their storage capacity. Even now that Colonial has announced the restart of its operations, it will take about 2 weeks for fuel from Houston to reach the east coast.

Petrol prices jumped 4% on Sunday 9th May and another 1.5% on Monday in response to the news. By 13th May, shortages had begun to multiply, and prices passed $3 per gallon for the first time in six years. Traders have begun booking deliveries from Europe by seaborne tanker.

The temporary spike in prices should be reversed as the pipeline comes back on line. European prices may be dragged upwards slightly because of the diversion of tankers. The fuel demand from the affected area should drop below normal for a few days as users draw down their precautionary stocks. Overall, the incident should cause only a slight hit to demand because of reduced driving.

Figure 2 Gasoline shortages by state during 10-12th May (Central US times)[v]



IMPLICATIONS

Cyberattacks cover a range of approaches and motivations. These include financial (ransomware, extortion), espionage (corporate or national), and sabotage (which could be by state, state-sponsored or non-state groups).

The oil and gas industry has been widely suspected to be lax on cybersecurity. Spending on security is low, operational systems are not always "air-gapped" (i.e. they can be connected to the internet, creating vulnerabilities), and in the US, they are regulated by several different agencies with only voluntary guidelines on cybersecurity. The energy industry in general, including electric grids, has also been a target (Table 2).

As large and wealthy companies operating critical infrastructure, energy companies are an obvious target for both profit-seeking and political-motivated cyberattacks. Attacks on control systems have to be more targeted and specialised than those on generic computer systems, but they have the potential to cause major physical damage.

Work-from-home practices during the pandemic have created additional vulnerabilities. Increasing levels of cloud data storage, remote work, automation, "smart homes", drones and internet-connected devices are attractive to the energy industry because of reduced costs, greater safety and enhanced data and capabilities. But they demand much-improved cybersecurity practices, that are not prone to human error and do not overload users. These include

Table 2 Notable cyber-attacks on energy companies and infrastructure [vi]

Date	Target	Actions	Motive
2010	Stuxnet attack on Iran	Destroy uranium enrichment centrifuges	Damage Iran's nuclear programme; US-Israeli operation
2012	US gas pipelines	Cyber-intrusions	Unknown
April 2012	National Iranian Oil Company	Data affected	Political?
August 2012	Shamoon attack on Saudi Aramco	Wiping data	Iran-backed, political?
August 2012	RasGas, Qatar	Systems offline	Unknown
December 2014	Korea Hydro and Nuclear Power	Data theft and disclosure	Political, North Korea?
December 2016	Industroyer attack on Ukraine power grid	1-hour blackout	Political, Russia-backed?
January 2017	Tasnee, Saudi petrochemical company	Systems offline	Political?
August 2017	Triton attack on Sadara, Saudi petrochemical company	Attempt to trigger explosion	Political?
April 2018	4 US gas pipeline companies	Disrupting customer service	Probing vulnerabilities, profit?
June 2019	Russian power grid	Unknown	Political, US retaliation
November 2019	Pemex, Mexico	Computer systems affected	Profit ($5 million ransom demanded)
December 2020	Solarwinds intrusion on US Department of Energy, other government bodies	Espionage	Russian espionage?
May 2021	Colonial Pipeline, US	Ransomware	Profit

biometric and multi-factor authentication, download restrictions, and need-only access. Key data should be saved in at least three locations, one of which is air-gapped.

But intrusions and cyber-attacks will always be possible, particularly against smaller or less well-resourced companies, and by sophisticated government-backed hacking operations with political motives. Current points of geopolitical tensions, such as US-Russia, Russia-Ukraine, US/Israel/GCC-Iran, North-South Korea, and US-China, are obvious points for state-directed hacks and cyberattacks. The level of deniability and difficulty of attribution makes cyberwarfare attractive for "grey zone" conflicts. State-directed hackers can claim to be acting for profit or for other political causes, or to be from entirely different countries, in order to misdirect possible retaliations.

In the case of a major escalation or an outright military confrontation, it's likely that cyber would be an immediate weapon. Highly networked societies, like the US and much of East Asia and Europe, are likely to be more vulnerable. Such cyberattacks could aim to cause major disruption, even serious damage and casualties, by attacking critical power grids, fuel lines, or facilities (such as natural gas processing plants, refineries, petrochemical plants and nuclear reactors), with explosive and toxic materials.

CONCLUSIONS

The long-term direct consequences of the Colonial Pipeline attack will not be very serious. Beyond some mild travel disruption, normal fuel supplies should be resumed within 1-2 weeks at most.

However, following various less-publicised cyberattacks, this incident should raise the urgency of improving the cyber-security of key energy infrastructure.

Vulnerabilities to cyberattacks will likely remain and should be expected to continue to rise, as energy systems become increasingly networked. A move to renewable energy may diminish some energy security risks, but it will greatly intensify reliance on the electric grid, for electric vehicles, industrial power, building heating and cooling and water desalination, as well as the current major uses for appliances and lighting.

This will require greater attention to all facets of energy security. The recent winter storms causing a major blackout in Texas, a non-cyber-related disaster, show that greater resilience is required across the whole energy system.

For instance, in the case of the US, the outdated Jones Act makes it much harder to move fuel by sea. Most of the US's Strategic Petroleum Reserve (SPR) is held at the Gulf Coast, while much fuel demand is in the north-east which has only a very small reserve. The SPR is also mostly crude, not refined products, which makes it of little use if refineries are shut down by a hurricane or a cyberattack. The fuel shortages in the Colonial incident have been exacerbated (even caused, in states such as Florida) by panic buying, which could have been limited by rationing or other measures.

The growing prevalence of both criminal and state-backed cyberattacks will lead to a greater attention, and spending, on energy companies' cybersecurity. But it should also merit an overall review of critical infrastructure and greater resilience and back-up to avoid single points of failure and cascading collapses. These vulnerabilities should also encourage a general attention to reducing conflicts where possible. In those senses, the Colonial Pipeline episode may turn out to have been a valuable warning - In other words, the episode could be some blessing in disguise by prompting the long overdue wakeup call.

APPENDIX

i. https://www.mckinseyenergyinsights.com/resources/refinery-reference-desk/colonial-pipeline/
ii. https://www.colpipe.com/news/in-the-news/colonial-pipeline-101-know-colonial
iii. https://www.bloomberg.com/news/articles/2021-05-10/white-house-creates-task-force-to-deal-with-pipeline-breach?sref=IUPsko0S
iv. https://cpcyberresponse.com/
v. Data from https://twitter.com/GasBuddyGuy
vi. Media reports

OUR PARTNERS

The Al-Attiyah Foundation collaborates with its partners on various projects and research within the themes of energy and sustainable development.

UİP-ICP
ULUSLARARASI İŞBİRLİĞİ PLATFORMU
INTERNATIONAL COOPERATION PLATFORM
İSTANBUL

World Petroleum Council

MITSUI & CO.

مؤسسة قطر
Qatar Foundation
Unlocking human potential لإطلاق قدرات الإنسان

KAHRAMAA
كهرماء
المؤسسة العامة القطرية للكهرباء والماء
Qatar General Electricity & Water Corporation

NATIONAL COUNCIL ON U.S.-ARAB RELATIONS

ISAG
Istituto di Alti Studi in Geopolitica e Scienze Ausiliarie

مجلس قطر للمباني الخضراء
QATAR GREEN BUILDING COUNCIL

جامعة حمد بن خليفة
HAMAD BIN KHALIFA UNIVERSITY

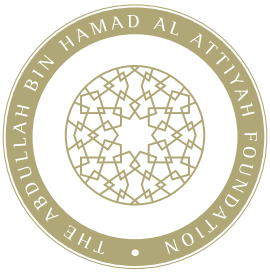
United Nations Global Compact

جامعة قطر
QATAR UNIVERSITY

COLUMBIA UNIVERSITY
IN THE CITY OF NEW YORK

GORD
المنظمة الخليجية للبحث والتطوير
Gulf Organisation for Research & Development

GULF TIMES



Barzan Tower, 4th Floor, West Bay, PO Box 1916 - Doha, Qatar

Tel: +(974) 4042 8000, Fax: +(974) 4042 8099
www.abhafoundation.org

AlAttiyahFndn
The Al-Attiyah Foundation