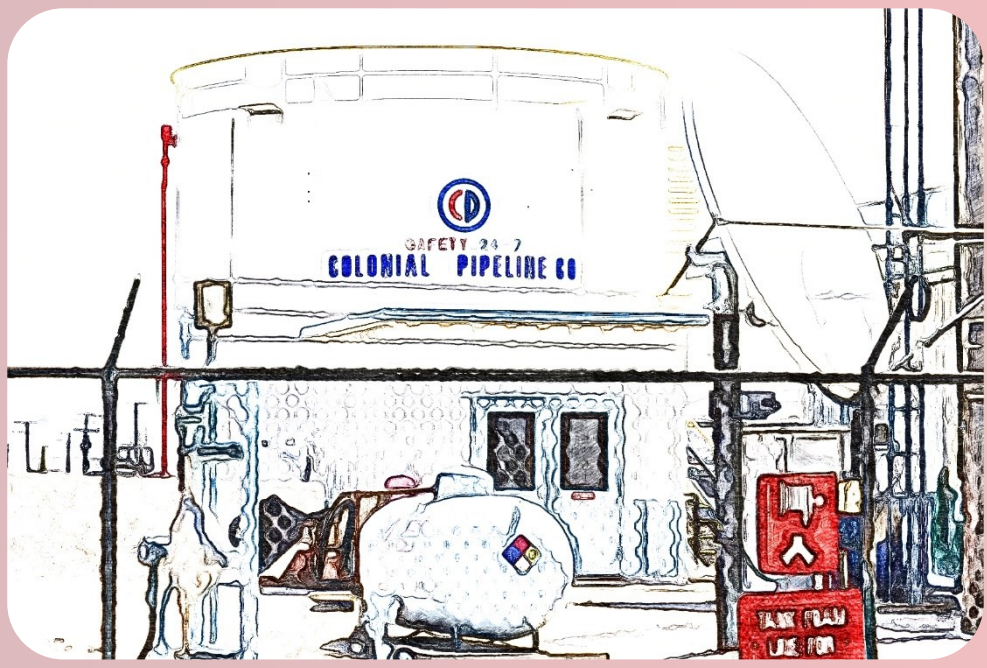
Colonial Pipeline Hack Highlights Growing Energy Security Risks

Infrastructure cyberattacks are a threat to national security



Max Pyziur

Lucian Pugliaresi

June 2021

ENERGY POLICY RESEARCH FOUNDATION INC.

EPRINC Est. 1944

© Copyright 2021
Energy Policy Research Foundation, Inc.
1031 31st Street, NW
Washington, DC 20007
- 202.944.3339
- eprinc.org

Introduction

U.S. energy security policy has its roots in the 1973-74 Arab oil embargo. As the embargo took hold, rising gasoline prices and petroleum product shortages that were exacerbated by price controls and government allocation programs acted to impose widespread economic damage to the national economy. Critically, the embargo highlighted U.S. vulnerabilities to both growing petroleum imports and geology; vast low-cost oil reserves were concentrated in an unstable part of the world. In response, the federal government undertook a wide array of policy measures over many years, which included the development of the Strategic Petroleum Reserve (storage for emergencies), promotion of more diversified sources of petroleum, expansion of domestic oil production, fuel efficiency programs, and the development of alternative energy sources. Many of these efforts bolstered U.S. energy security.

But unforeseen at the time, a combination of technological innovations began being applied to oil and gas exploration and production in the 1990s. This has led to a rapid expansion of unconventional oil and gas production over the last twenty years from domestic resources, and has also caused U.S. net petroleum imports to drop to zero. In the process, it has muted and even removed the sense of vulnerability to foreign sources of energy.

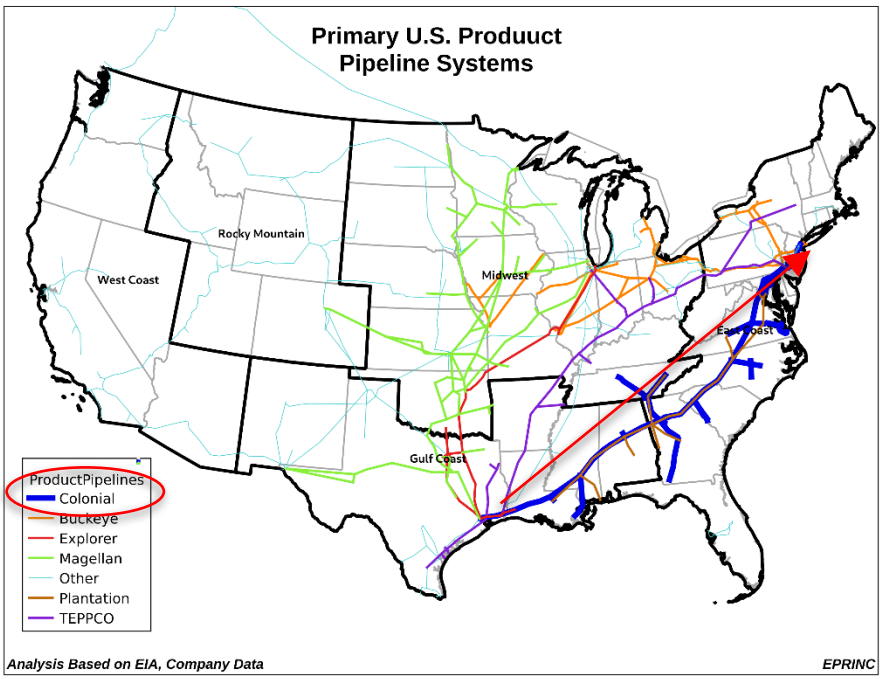
The recent hack of the Colonial Pipeline computer systems, which disrupted gasoline supplies to the Northeast has raised a new set of energy security concerns. Although the attack was presumably not the actions of a state entity, it is hard not to view it as an act of terrorism given its potential for widespread disruption. This is not a new threat. In the late 1990s, President Clinton issued Presidential Directive 63 which recognized that growing threats to critical infrastructure had become "increasingly automated and interlinked." The Directive mandated that within five years (by 2003) critical U.S. infrastructure would be hardened to cyberattacks. Despite the Directive, measures to protect infrastructure from growing cyberattacks have not kept up.

Anatomy of a pipeline hack

On Friday May 7, 2021, the Colonial Pipeline system was the victim of a cyberattack in the form of ransomware. The target was one of Colonial's billing and customer communication systems. Nevertheless, as a precaution, the whole pipeline system was shut down so that a full analysis of the scope of the attack could be done. This was one of the most consequential ransomware attacks ever on any piece of U.S. energy infrastructure impacting one third of the United States.

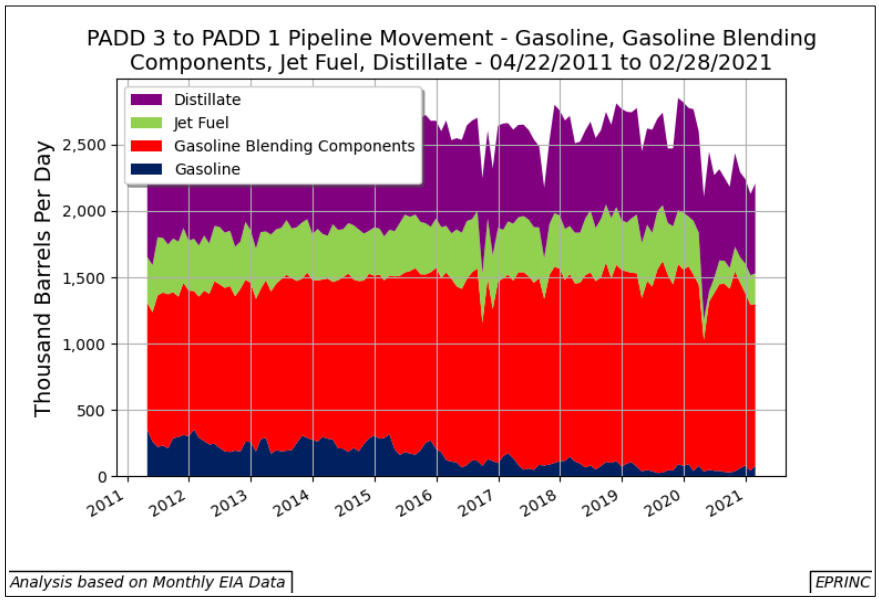
Commissioned in 1964, the Colonial Pipeline (*Figure 1*) is the largest petroleum product pipeline network in the U.S. It moves up to 2.5 million barrels per day (MBD) (*Figure 2*) through 5.5 thousand miles of intertwined pipelines from the U.S. Gulf Coast refineries to product terminals located in the Southeastern, MidAtlantic, and Northeastern parts of the U.S.

Figure 1



The Colonial is one of six large product pipeline systems that collectively move petroleum products such as gasoline and diesel from producing centers in the U.S. Gulf Coast and Midwest to consuming centers located between the Atlantic Coast and the eastern slopes of the Rocky Mountains. The operations of product pipelines are distinct from other types of pipelines such as those crude oil and natural gas. Rather than moving only one type of commodity, product pipelines sequence their commodities in specific ways with one product pushing another product with methods established to deal with any comingled fuel.

Figure 2



The U.S. Atlantic Coast consumes almost 6 MBD of petroleum products. Due to limited regional production capacity, a large

portion of this comes from other parts of the U.S., especially the Gulf Coast, and in particular the Colonial system.

Rather than being initiated by a state-sponsored entity, the FBI has ascertained that the attack came from DarkSide, an entrepreneurial ransomware hacking group based in Eastern Europe, most likely Russia.

Recognizing the magnitude of this event, the Biden Administration, led by the Department of Energy, quickly setup an interagency group to find ways to manage the situation. The attack comes at a critical point on the cusp of an economy trying to recover from COVID, and ahead of summer driving.

While some major price impacts had materialized across the served region, more critically due to hoarding, large scale shortages developed in states such as Georgia, North and South Carolina, and even the District of Columbia where many, if not most, filling stations had no fuel to sell. At the peak of this crisis the number of stations without fuel reached a peak of over sixteen thousand.

Colonial announced that it had paid $5 million in ransom just after the attack using cryptocurrencies. In response, DarkSide sent decryption software in order for Colonial to restore its hijacked data. However due to the slow rate of decryption along with the verification of the integrity of the rest of its IT components. Colonial did not begin restarting the system until five days later, Wednesday May 12, 2021. Given the scale and scope of the impact, along with its size and with fuel products moving at a rate of between 3 to 5 MPH, it will take some time to replenish terminals and other facilities along the network. As an example, gasoline injected into the system at Houston TX will take about 2 1/2 weeks to reach New York harbor.

Reliance on information systems to manage and automate expansive infrastructure, energy and otherwise, has been increasing with time, even more so with the onset of the Internet in the 1990s. Concurrently, this has created large opportunities for hackers.

While the reporting of cyberattacks on critical U.S. infrastructure assets has gained notoriety in recent times, this threat was recognized still in the late 1990s as the Internet began to expand into commercial realms. Importantly, President Clinton's Administration issued Presidential Decision Directive 63 (PDD 63) on May 22, 1998. Recognizing that,

"... Many of the nation's critical infrastructures have historically been physically and logically separate systems that had little interdependence. As a result of advances in information technology and the necessity of improved efficiency, however, these infrastructures have become increasingly automated and interlinked. These same advances have created new vulnerabilities to equipment failures, human error, weather and other natural causes, and physical and cyberattacks. Addressing these vulnerabilities will necessarily require flexible, evolutionary approaches that span both the public and private sectors, and protect both domestic and international security."

At the time representing some of the energy interests advising the crafting of PDD 63 was Larry Goldstein, then President of PIRINC, EPRINC's predecessor and a Board member of the National Petroleum Council. Presidential Directive 63 emphasized that, " .

No later than the year 2000, the United States shall have achieved an initial operating capability and no later than five years from the day the President signed Presidential Decision Directive 63 the United States shall have achieved and shall maintain the ability to protect our nation's critical infrastructures from intentional acts that would significantly diminish the abilities of:

the Federal Government to perform essential national security missions and to ensure the general public health and safety;
state and local governments to maintain order and to deliver minimum essential public services;
the private sector to ensure the orderly functioning of the economy and the delivery of essential telecommunications, energy, financial and transportation services."

2003, the deadline set in PDD 63, has passed a long time ago. Federal cyber oversight authority and enforcement has developed but diffused across a loose quilt of agencies. Despite that, cyberattacks have been ongoing and continuing to increase in their number, scale, and criticality.

Following the Colonial ransomware cyberattack, calls have again resumed for increased vigilance and preparation have come from members of the U.S. Congress. Already, Congressional Committees have announced that this event will be a key component of upcoming hearings.

Cyber Threats Affect a Broad Range of Realms

Operations

Cyberattacks are not knew or uncommon. Beginning in the middle of the 1990s, they have been part of the cyber terrain when the Internet moved away from just serving academic computer labs to becoming commercial. Ransomware was conceptualized during this very period; however, it was not until 2005 that its extortionist use became prominent and elevated. Most ransomware has targeted relatively small but lucrative systems: IT systems of entities such as hospitals and municipal or state governments. The combination of relatively isolated smaller systems along with poorly trained support staff have made these systems easy targets for hackers having one or two degrees higher in computer skills.

In recent years, cyberattacks targeting energy infrastructure systems have caused disruptions. But these have been mostly limited to things such billing or customer communication systems, not directly affecting operations.

With increased reliance on computerization to manage control systems and critical infrastructure and using the internet to connect devices (such as compressor stations, gauges) dispersed geographically, increased vulnerabilities are created. Unless systems are hardened and administrators are vigilant to existing and increasing threat levels, attacks and compromisations become almost inevitable. The Colonial cyberattack, however, just elevated the awareness and scale of these possibilities because the size of the assets are so large, and the response, both operationally on the company side as well as the reaction of fuel consumers, was huge.

Oversight, Regulation, and Jurisdiction

In Congressional testimony given in 2019, Dan Coats, the Director of National Intelligence at the time, identified energy pipelines as having cyber vulnerabilities that, if exploited successfully, could lead to shutdowns lasting for extended periods of up to several weeks. However, these were not the first warnings given at this high of an oversight level. The first were offered as early as 2003.

Response plans to major national cyberattacks, whether as ransomware or some other form, have been formulated by several agencies including the National Institute of Standards and Technology (NIST), the FBI, and Cybersecurity and Infrastructure Security Agency (CISA). Generally and depending on the severity, these responses are prescribed in the National Cyber Incident Response Plan, and are to be led by a Unified Coordination Group. But since the Colonial incident targeted one company and it involved energy, the response is deemed to be led by the Department of Energy.

However, in the case of cyberattacks on interstate pipelines, specific regulations and jurisdictions are complicating factors. While the Department of Energy is leading the cyberattack response, different pipeline types fall under different legislation and oversight and enforcement authorities. PHMSA (Pipeline and Hazardous Materials Safety Administration, an agency of the Department of Transportation) has authority over pipeline safety. FERC (Federal Energy Regulatory Commission) has responsibility for overseeing rates charged for interstate pipeline energy transportation. Environmental spills are under the authority of EPA. But security is the responsibility of the TSA (Transportation Security Administration, an agency of the Department of Homeland Security).

By the enactment of the Implementing Recommendations of the 9/11 Commission Act of 2007, the TSA is authorized to promulgate pipeline security regulations, and to carry out necessary inspections and enforcement. Unlike FERC and interstate electricity transmission where FERC determines and enforces explicit cyber standards on grid operators, TSA only has issued voluntary guidelines for pipelines' physical and cybersecurity since the passage of the 9/11 Act. TSA together with the pipeline industry have maintained that regulations are unnecessary since pipeline operators claim that that their security programs have been sufficient.

Adding to the inadequacy of voluntary guidelines is the small staff size that TSA dedicates to this set of concerns. Until fiscal 2020, TSA had six people dedicated to security; the 2020 budget resolution expanded this to thirty-four with twenty mandated to receive special cyber training. Still the oversight has remained suggestive rather than mandatory.

Critically and in bipartisan fashion, current FERC Chairman Richard Glick (a Democrat) and former FERC Chairman and current Commissioner Neal Chatterjee (a Republican) have jointly authored editorials as well as made other announcements raising concern regarding physical and cybersecurity concerns relating to U.S. interstate pipelines.

With the glaring inadequacy of the loose quilt of agencies, divisions of oversight, and jurisdictions dealing with cybersecurity coupled with the tailwinds coming from the Colonial cyberattack following other previous events, certain pipeline security legislative initiatives have been either newly presented or renewed. Notably, Congressman Emanuel Cleaver's (D-MO) 2021 Pipeline Security Act has been resubmitted to the House Homeland Security Committee for markup; the focus is to reinforce the TSA

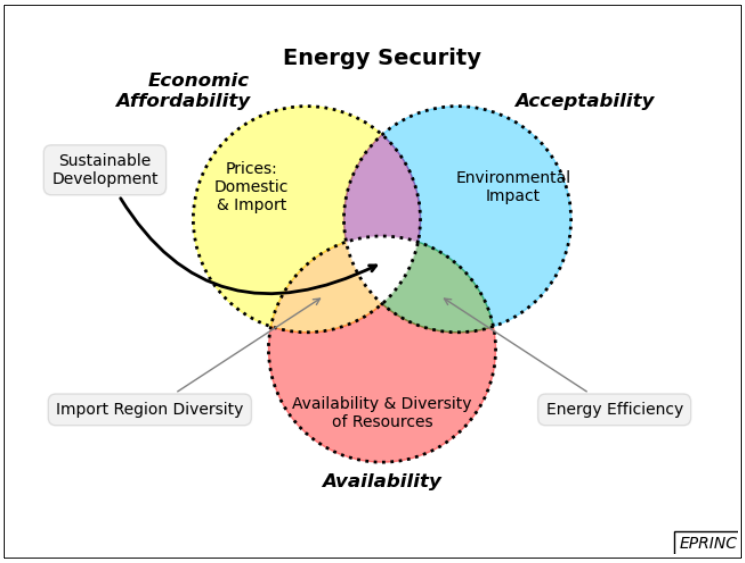
as well as to increase its level of authority. In addition, the Energy Subcommittee (of the House Energy & Commerce Committee) is debating a new bill putting the Department of Energy in charge of pipeline as well as LNG cybersecurity. Other Members of Congress have sponsored measures would expand cybersecurity oversight to include other types of infrastructure.

On the U.S. Senate side, Senate Commerce Committee Chairwoman Maria Cantwell is calling for consolidation of pipeline oversight. Echoing Senator Cantwell, Senator Joe Manchin, Chairman of the Senate Energy and Natural Resources, sees opportunities for streamlining and strengthening of pipeline oversight and regulatory enforcement.

Cybersecurity as Energy Security

Energy Security: it is a multifarious concept (see *Figure 3* for the key components) used more intuitively rather than in specific formal terms. Formally, it involves overlapping concepts of economic affordability, acceptability, and availability. At points where these concepts overlap, there are additional notions of import vulnerability, efficiency, and sustainable development.

Figure 3



Beginning in the 1970s with curtailed oil supplies and elevated political tensions, the U.S. developed a collective sense that reliance on imports created considerable vulnerability and exacerbated economic affordability. While largely unproclaimed, that sense of energy insecurity has been mitigated and essentially removed with the North American Petroleum Renaissance that came on the heels of new hydrocarbon exploration and extraction techniques. With a resurgence in North American production, fear of foreign dependency has been almost eliminated.

Conclusion

Dominating its political agenda, the Biden administration is pursuing an aggressive program to reduce U.S. emissions of greenhouse gasses (GHGs). This program will not only commission large scale investments in carbon capture systems and alternative fuels, but also will require highly integrated and complex solutions to ensure resilience of supply chains and sustained operation of power and transportation sectors. Given these policies, the production and distribution of American energy is about to get a lot more complex as dependence continues to grow on information processing and dispersed computer networks to ensure reliable operation of transportation systems and generation and distribution of electric power, much of it from intermittent sources.

The American public has a history of not paying much attention to energy policy except when fuel sources are disrupted or prices surge. That tolerance has a limit as at least two California governors from the last twenty years can testify. There is a heavy political penalty for failure to keep the lights on.

Massive electrification of the national economy will be expensive, involve large technical risks, and may also give us a much less secure energy complex. These risks have to be part of the national discussion of the energy transition.