CANADIAN GLOBAL AFFAIRS INSTITUTE
INSTITUT CANADIEN DES AFFAIRES MONDIALES

Colonial Pipeline Cyber Attack

by Ben Huang

July 2021

CONFERENCE REPORT

COLONIAL PIPELINE CYBER ATTACK

by Ben Huang

July 2021

CANADIAN GLOBAL AFFAIRS INSTITUTE
INSTITUT CANADIEN DES AFFAIRES MONDIALES

Prepared for the Canadian Global Affairs Institute
1800, 150 – 9th Avenue S.W., Calgary, AB T2P 3H9
www.cgai.ca

Ellen Wald – President, Transversal Consulting

Ken Barker – Professor of Computer Science, University of Calgary

Chuong Dong – Computer Science Student, Georgia Institute of Technology

Energy security in the digital age means more than just securing domestic sources of energy. On May 7, 2021, the Colonial Pipeline, the largest refined oil products pipeline in the United States, was hit with a ransomware attack from the criminal hacking group DarkSide. This attack forced the Colonial Pipeline to shut down and prompted U.S. President Joe Biden to declare a state of emergency to allow fuels to be transported by road. Regardless, the six-day pipeline shutdown resulted in fuel shortages in Alabama, Florida, Georgia, North Carolina, and South Carolina. While stopping a pipeline in the past might have required a bomb, it can now be done with an email.

***QUESTION**: How prepared is the U.S. for additional cyberattacks targeting energy infrastructure?*

Ken Barker

- There is far less security than we expect. Cybersecurity is a complex issue, which has been there for years. Since the information systems for infrastructure are old, they are more vulnerable to being cyberattacked. There are two levels of attack: IT system and operation. First, the IT system in the infrastructure can be vulnerable. When an IT system is attacked, there might be a denial of services. After that, there will be a loss of control of the operation.

- Although a new system can be applied to the old system, the system addition posts new vulnerabilities for cyberattacks. This complexity can be applied to every sector, such as hydro, nuclear, etc.

Ellen Wald

- This event is a wake-up call to understand the weakness of cybersecurity in energy infrastructure. The U.S. is not prepared in a holistic way. The systems designed for cybersecurity do not work cohesively to prevent cyberattacks. There is a lack of a universal system-wide protocol to encounter situations of cyberattacks.

- There are no preparation plans to address each scenario with the proper response. Once a cyberattack occurs, an immediate solution that can be drawn from the preparation plans should be proposed to reduce further damage to the system.

Ken Barker

- There are concerns about preparation plans.

- People often fail to implement the preparation plans after the situation really happens. The reality is usually different from what we have expected and prepared. For example, governments all have pandemic plans but end up not using them.

- A retroreflective method is suggested to increase prevention mechanisms to reduce the risks of cyberattacks.

Chuong Dong

- This cyberattack sheds light on the cybersecurity issues facing energy infrastructure. There are three stages of being cyberattacked. The first is to obtain initial access to the system. The second is to inspect the system and potentially steal as many files as possible. The third is to drop the ransomware and ask for payment.

- As many people have a working from home setup, the workstation can be an easy gate to have initial access. For a lot of people, they might not have well-rounded protection on their devices and might use a simple password to login.

***QUESTION**: What was the worst-case scenario for the Colonial Pipeline if DarkSide had darker motives?*

Ken Barker

- There are a hundred thousand of devices and sensors in the pipeline. If any of them does not function as planned, there will be serious problems.

    - For example, if a leak detector stops to work (a valve opens upstream and the other closes downstream), an explosion might happen. If it is in a populated area, it can become a dangerous terrorist attack. The hackers can threaten to blow up cities after cities, leading to huge cost and loss of faith in national security.

- Old systems are more vulnerable to this type of cyberattack. Even if it is new now, it will be old in the future, adding up the vulnerability of energy infrastructure to cyberattacks.

***QUESTION**: Does the Colonial Pipeline shutdown demonstrate that energy infrastructure is more vulnerable to cyber disruption?*

Ellen Wald

- Energy infrastructure is vulnerable to cyberattacks because you cannot monitor what is happening there in the pipeline. After a cyberattack, the only thing you can do is to shut down the operation. The situations in the pipelines can be detrimental to a large population. It is safer to take extra precautions to reduce risks. For cyberattacks on other subjects, they can recover quickly as they do not worry about those extra risks.

***QUESTION**: Will this event open the conversation in cybersecurity and indeed promotes more attention and changes to cyberattack prevention?*

Ken Barker

- Governments are realizing the importance of cybersecurity. Canada is planning to spend a large amount of money on cybersecurity issues. Biden intends to invest in the research of cybersecurity. We should see positive moves as we are on the right trajectories. However, this might not trigger significant changes regarding the protection and prevention from cyberattacks.

Ellen Wald

- Responsibilities of cybersecurity issues should be moved to the department of energy as they will be better prepared if an energy infrastructure cyberattack occurs.

***QUESTION**: With more protection, will those hackers be encouraged more to prove their abilities to perform cyberattacks?*

Chuong Dong

- There is no way we have perfect security. There will always be a cyberattack. However, getting through the initial access is time-consuming work. It is not worthwhile to prove this if it is not for money.

Ken Barker

- At the University of Calgary, we have around 6,500 cyberattacks a day. We even had a 10-week lockdown of our systems before. If more protection attracts cyberattacks, the reverse will also be true. Then if we open completely, nobody wants to attack. This is incorrect. Attacking and defending is an endless game for cybersecurity issues.

***QUESTION**: How can individuals deal with a cyberattack?*

Ellen Wald

- Change your passwords frequently.
- The cyberattacks should be discussed openly to inform the public and improve the cybersecurity strategy for everyone.

***QUESTION**: How much of the fuel shortage can be attributed to the real effect of the pipeline shutdown, and how much to public hysteria? What does this mean for energy security?*

Ken Barker

- Hoarding and overreacting in this case is part of human nature. For example, when the pandemic just began, people were hoarding toilet paper. It is in human nature that people want to overreact to this situation.

Ellen Wald

- This is panic buying. One of the reasons why there is a fuel shortage is the shortage of truck drivers. This exacerbates the fuel shortage and causes panic buying.
- The public message is important to help manage the panic buying. Also, regulations on purchase can be useful to discourage panic buying.

CLOSING COMMENTS

Ken Barker

- We should understand we can design a resilient system to prevent future cyberattacks. From the operational aspects, we should have backup files so that we can easily restore the operation by identifying the hole and reloading the system. From IT system aspects, we should design a system that addresses the fundamental flaws of cybersecurity. Then we can respond to cyberattacks properly.

Ellen Wald

- We need to be aware of the cybersecurity issues, and we should also realize how important the pipelines are in our daily activities. It is an efficient way to manage energy resources, and it is key to our society's operations.

This report was funded in part by a grant from the United States Department of State. The opinions, findings and conclusions stated herein are those of the speakers and do not necessarily reflect those of the United States Department of State

About the Author

Ben Huang *is working on his Master of Public Policy at the University of Calgary. He received his BA (2020) with a double-major in Economics and Sociology from the Acadia University, in Nova Scotia, completing an undergrad thesis on microcredit policy. Ben is a member of the World University Service of Canada. In his spare time, Ben volunteers in community and outreach organizations.*

Canadian Global Affairs Institute

The Canadian Global Affairs Institute focuses on the entire range of Canada's international relations in all its forms including (in partnership with the University of Calgary's School of Public Policy), trade investment and international capacity building. Successor to the Canadian Defence and Foreign Affairs Institute (CDFAI, which was established in 2001), the Institute works to inform Canadians about the importance of having a respected and influential voice in those parts of the globe where Canada has significant interests due to trade and investment, origins of Canada's population, geographic security (and especially security of North America in conjunction with the United States), social development, or the peace and freedom of allied nations. The Institute aims to demonstrate to Canadians the importance of comprehensive foreign, defence and trade policies which both express our values and represent our interests.

The Institute was created to bridge the gap between what Canadians need to know about Canadian international activities and what they do know. Historically Canadians have tended to look abroad out of a search for markets because Canada depends heavily on foreign trade. In the modern post-Cold War world, however, global security and stability have become the bedrocks of global commerce and the free movement of people, goods and ideas across international boundaries. Canada has striven to open the world since the 1930s and was a driving factor behind the adoption of the main structures which underpin globalization such as the International Monetary Fund, the World Bank, the World Trade Organization and emerging free trade networks connecting dozens of international economies. The Canadian Global Affairs Institute recognizes Canada's contribution to a globalized world and aims to inform Canadians about Canada's role in that process and the connection between globalization and security.

In all its activities the Institute is a charitable, non-partisan, non-advocacy organization that provides a platform for a variety of viewpoints. It is supported financially by the contributions of individuals, foundations, and corporations. Conclusions or opinions expressed in Institute publications and programs are those of the author(s) and do not necessarily reflect the views of Institute staff, fellows, directors, advisors or any individuals or organizations that provide financial support to, or collaborate with, the Institute.