To what extent do cyberattacks on the US affect American public trust in government?

By Anna Lysenko

Thesis: **Cyberattacks on the US decrease American trust in government by making people question their belief in the state's ability to protect them from new threats to infrastructure, food security, and privacy.**

Methodology: Online secondary sources, including news articles and polls, were used to research cyberspace, cyberattacks, and the three case studies. Books and academic articles were used for analysis and implications.

1) Infrastructure: the Colonial Pipeline (CP) attack

- The CP is the **largest refined oil pipeline system** in America. On April 29th, 2021, hackers gained access to the digital pipeline system due to a **single compromised password**. The breach was noticed by an employee on May 7th after a **ransom note** demanding **cryptocurrency** appeared on a computer screen. The pipeline was shut down within an hour.
- On May 8th, Colonial announced it would pay the 4.4 million USD ransom, but operations would take a few days to restore. This led to **nationwide consumer panic and gas prices rising**. President Biden made an announcement lifting all limits on amounts of domestic gas transportation to lower gas prices and calm the public. In the aftermath of the attack, it was reported that around **100 gigabytes of employee data were stolen**.

2) Food Security: the JBS attack

- JBS SA is one of the four **largest meat companies in the world**. On May 30th, workers in JBS factories across the world got a **ransom note** on their devices, demanding **cryptocurrency** payment in exchange for control of various beef and pork slaughterhouses in America, Canada, and Australia. The hackers did not damage equipment but warned they **could damage delicate systems** if the ransom would not be paid promptly.
- JBS shut down all slaughterhouse, meatpacking, and shipping systems, leading to the **number of cattle slaughtered in America dropping by 22% for a week**, and the **price of American beef rising around 1%**. On June 9th, a JBS spokesperson stated that JBS would pay the 11 million USD ransom to get back system control. There were no reports of data being stolen.

3) Privacy: the SolarWinds data breach

- The SolarWinds data breach **targeted** vast parts of the American government and private sector. The attack began as early as March 2020, with hacker actions being traced back to as early as September 2019. Malicious code was **distributed through a routine software update** package of Orion, a popular network-monitoring application. Nearly **18,000 users** installed the malicious update, including actors in **key federal agencies**, from the Department of Homeland Security to the the Department of Energy, the agency that oversees America's nuclear weapons arsenal.
- The **Russian** group CozyBear was suspected to be behind the attack, with the likely motive being **cyberespionage** for the Russian government. While affected actors did their best to restore protection by reupdating systems and changing passwords, experts are **still uncertain** about whether the hackers have some **access to systems through digital backdoors**.

Implications:

All three cases demonstrate the **cyberattack's versatility and damage to trust in the government**. In the CP case, rising oil prices created **national anxiety**, and questions about **government competence** in protecting Americans from cyberattacks. Similarly, in the JBS case, the meat industry realized its **vulnerability** to cyberattacks and had to consider how the government could **confront the attackers responsible**. Finally, the government itself was one of the targets of the SolarWinds breach, leading to **direct questions about the government's cybersecurity posture**, and plans to improve cybersecurity. In all three cases, Americans witnessed their government's lackluster cybersecurity approach and questioned whether they could trust their government to protect them from **future cyberattacks** and **mitigate other rising security threats**.

Potential Solutions:

Improving American cybersecurity and repairing public trust in government requires the government to undergo a **paradigm shift** in its understanding of cybersecurity; the government still approaches cybersecurity as a slow, growing threat that awaits culmination, but cybersecurity presents a much more **dynamic, ground-level challenge**. To improve America's cybersecurity approach, the **bureaucracy** must be adjusted for increased **cross-departmental communication**. The government should be upfront about previous weaknesses with the public and **collaborate with the private sector** for improvement. The government should also take on a **sterner geopolitical approach** to malicious actors behind cyberattacks. **Public cyberattack attribution**, paired with **sanctions and diplomacy** would serve as effective deterrents. Finally, **more research** on the effects of cyberattacks on politics, and of the future of cyberspace, is necessary to construct clearer solutions and enhance America's force in the field.

LAIDLAW FOUNDATION

I am immensely grateful to the Laidlaw Foundation and Lord Laidlaw for allowing me to pursue this research and to my supervisor Dr Joy Fitzgibbon for her unwavering support and advice.

UNIVERSITY OF TORONTO