C-SPAN: Select Committee Hearing on China’s Cyber Threat to the U.S

Jasmine Roberts

Bowie State University

CTEC-335-102-SPRG2024

April 7, 2024

C-SPAN: Select Committee Hearing on China’s Cyber Threat to the U.S

On January 31, 2024, the Select Committee Hearing on China’s Cyber Threat to the U.S. addressed concerns surrounding the cybersecurity of the United States and its infrastructure originating from China. As this remain as a lingering issue that would potentially cause severe chaos, the committee goes through many threats that previously happened and the current threats that are currently in motion. The hearing aimed to discuss and mitigate China’s cyber capabilities such as the CCP, which means the Chinese Communist Party. The CCP seeks control over people’s lives economically, politically, and physically by any means possible.

# **Testimony**

The Select Committee consisted of top officials that testified. An FBI director, Christopher Wray, National Cyber Director Harry Coker, and National Secuirty Agency Director Gen. Paul Nakasone they testified on behalf of China’s cyber threat to the U.S. homeland and national security before the House Select Committee on U.S. – China Competition. In general, for over 20 years the CCP has been attacking the U.S such as the government, defense contractors and technology firms in cyber space which led the attacks to be focused on theft of valuable technology. They gathered sensitive information of millions of Americans such as the Anthem Health Office of Personnel Management, which resulted into military records being compromised. China’s vast hacking program is the largest to date, they have stolen more American business and personal data more than any other nation.

To prove that China contiguously targets the U.S and that this has happened before, the committee described four men of the Chinese decent; Wang Dong, Sun Kailang, Wen Xinyu, Huange Zhenyou, and Gu Chunhui were indicted in 2014 and wanted by the FBI of conspiring to commit computer fraud, accessing a computer without authorization for the purpose of commercial advantage, and private financial gain, damaging computer through the transmission of code and commands, aggravated identify theft, economic espionage, and theft of trade secrets. Although, CCP used cyber operations to steal IPs from companies, collecting private citizens data, and hacking into government emails.

**Chinese Communist Party**

Although, CCP used cyber operations to steal IPs from companies, collecting private citizens data, and hacking into government emails. Secondly, fast forward to why this hearing was put in place. As stated, it was concerns that were addressed surrounding the cybersecurity of the United States and its infrastructure originating from China. The hearing was held on January 24, 2024, and the attempt from China happened last May. These threats from China include, putting the citizens of the U.S safety in jeopardy, trying to gain control of water treatment plants, electrical grid, oil and natural gas pipelines, and transportation systems. They are mostly focused on civilian infrastructure, low blows against civilians are a part of China’s plan. Another way the CCP tries to commit theft is to construct an alliance with people who work for these companies which would classify the workers as insiders.

For the CCP to commit any threat, they created the “Volt Typhoon” malware, which enabled them to attempt to hide their exploitations/crimes. This is like the PRC Threat acter which is the People’s Republic of China Cyber Threat, and it was named by a sector of the “Volt Typhoon”. The CCP attempted to attack Texas’s electric grid to install malware and once that malware is activated it will damage their infrastructure. An attack on an electrical grid would be the cause of losing access to cell towers, blackouts in cities and the internet, clean water, and fuel. The main goal was to disrupt the peace and military’s ability to mobilize, and to impact the system(s) that allow the U.S. to thrive digitally.

***Mitigation***

The Select Committee suggested ways of mitigation that would be sufficient of keeping threats at a minimum and hopefully to not come about at all. Mitigations include hunt and destroy malware ( “Volt Typhoon” and “People’s Republic of China Cyber Threat Actor”), all malicious code that the CCP is attempting to hide within the U.S. networks and infrastructure. The FBI were authorized to remotely disable aspects of the CCP hacking campaign to protect our network and devices. Also, self-defense would be put into use if the CCP activated code that would cause harm. Lastly, Present Biden’s National Cybersecurity Strategy was put in place the build and enhance collaboration to collectively defend against and respond to cyber threats from authoritarian states that go against our national interests. The strategy consists of five bullet points, one is to Defend Critical Infrastructure, two is to Disrupt and Dismantle Threat Actors, three is to Shape Market Forces, four is an Interest in a Renitent Future, and five is to Forge International Partnerships to Pursue Shared Goals.

*Conclusion*

In conclusion, Harry Cooker expressed that to elevate the CCP is to enforce the National Cyber Secuirty Workforce Education strategy which includes four pillars. The pillars include Equip Every American with Foundational Cyber Skills, Transform Cyber Education, Expand and Enhance Americas Cyber Workforce, and Strengthen the Federal Cyber Workforce. Also, expanding the Federal and Cyber Workforce as in availability for jobs. Ban or force the sale of Tik Tok, which they believe to be controlled secretly by the CCP, but they denied the allegations. Also, I believe we need to strengthen the nations knowledge on Cyber Secuirty and getting them aware on how bad this attack is on our National Secuirty.

# Works Cited

*C-SPAN*. (2024, January 31). Retrieved from Select Committee Hearing on China's Cyber Threat to the U.S : https://www.c-span.org/video/?533196-1/select-committee-hearing-chinas-cyber-threat-us

Poremba, S. (2023, May 2023 9). *The Biden administration’s 2023 cybersecurity strategy*. Retrieved from Security Intelligence: https://securityintelligence.com/articles/the-biden-administrations-2023-cybersecurity-strategy/

PRESIDENT, O. O. (2023 , July 31). *NATIONAL CYBER WORKFORCE AND EDUCATION STRATEGY*. Retrieved from NCWES-2023: https://www.whitehouse.gov/wp-content/uploads/2023/07/NCWES-2023.07.31.pdf