Political Implications of United States Cyber Deterrence Strategy Against China

Joey Navarrete

Old Dominion University

CYSE/POLS 425W: Cybersecurity Strategy and Policy

Professor Lora Pitman

March 26, 2023

The United States and China have had high tensions between each other ever since the People's Republic of China was established in 1949. With the increase in the use of technology in the 21st century, these tensions have also carried over into the cyber world. Not only are the United States and China using cyberspace with the intention of defeating each other, but both nations are looking to strengthen in power. Since the start of the millennium, the United States government has been in a constant search to weaken the cyber capabilities of China. This is known as cyber deterrence. The ongoing cyber deterrence strategy against China comes down to the current politicians within the governments of the United States and China.

The United States' cyber deterrence against China is the result of cyber warfare. This cyber warfare between the two nations is occurring because both nations have detected malicious instances of cyber activity. The United States' cyber deterrence strategy against China was enhanced in aggressiveness during the presidency of former President Barack Obama in response to an increase of cyber capabilities by China. This aggressiveness continued during the Trump administration as the relations between the United States and China were challenged by the trade war, the blocking of technology against China, and especially the COVID-19 pandemic (Lu & Xu, 2021). With the Biden administration taking control of the White House in 2021, their cyber deterrence policy against China remained relatively the same and are still looking to keep a high level of competition against China in cyberspace. As for China, they are responding to the United States' cyber deterrence policy by developing a cyber deterrence policy of their own in response to the "further development of cyber deterrence by the US" (Jiang, 2019).

There must be a reason why politicians and policy makers are overwhelmingly supportive of cyber deterrence against China. It appears that one of the primary reasons why the United States government is committed to carrying out their cyber deterrence policy against China is

because of China's constant offensive use of their cyber capabilities and the frequent cyber-attacks detected by the United States. With China being one of the strongest nations in the world in cyber offense, it was important for them to level the playing field with the United States and have a cyber deterrence strategy of their own because offensive power is all they were capable of. There are three principles of successful cyber deterrence that the United States government keeps in mind and why they support the idea of continuing the use of cyber deterrence. The first principle is attribution. In this principle, the United States government must know who carried out the cyber attack before implementing a counterattack (Iasiello, 2014). The next principle is repeatability, which is brought up when determining if the same type of strategy should be used. Cyber deterrence strategies are typically different depending on who or what the target is. The last principle for successfully using a successful cyber deterrence strategy according to the United States government is success. This principle is taken into consideration when figuring out if the deterrence was truly effective, as well as if more possible attacks are on the way (Iasiello, 2014). Politicians and policy makers in the United States have a strong understanding of how cyber threats can affect their country. The cyber threats posed against the United States against China are part of the reason why cyberspace is considered a domain.

Lastly, it needs to be understood that the United States government implementing cyber deterrence against China, or virtually any nation, could have significant ramifications. One major impact because of the United States' cyber deterrence strategy against China would be the weakening of relations between the two nations. With China being aware of the United States' response to their cyber-attacks, China could potentially become more aggressive in their intentions to launch cyber-attacks against the US. Another impact of implementing cyber deterrence against China is the effect it could have on the economy. Cybersecurity in the United

States is rather expensive, and it could cost much more when being used for cyber deterrence. On the other hand, using cyberspace for offensive capabilities are not nearly as expensive. Along with being easy to implement, offensive cyber operations, including cyber-attacks, are “low cost, covert, but extremely destructive” (Jiang, 2019).

The United States policy of cyber deterrence against China has many implications, the largest implications coming from the political world. As of 2023, the United States remains aggressive in their cyber deterrence strategy against China. The politicians within the United States are in agreeance with the cyber deterrence strategy because they understand China’s offensive cyber capabilities and want to help the United States in its cyberspace endeavors. Though there are some massive risks with this cyber deterrence strategy, the United States government must protect their nation from any potential cyber threats from China.

References

Iasiello, E. (2014). Is Cyber Deterrence an Illusory Course of Action? *Journal of Strategic Security*, *7*(1), 54-67. https://www.jstor.org/stable/26466501?seq=16

Jiang, T. (2019). From Offense Dominance to Deterrence: China's Evolving Strategic Thinking on Cyberwar, *Chinese Journal of International Review*, *1*(2), 1-23. https://www.worldscientific.com/doi/pdf/10.1142/S2630531319500021

Lu, C. & Xu, M. (2021). China-U.S. cyber-crisis management, *China International Strategy Review*, *3*, 97-114. https://doi.org/10.1007/s42533-021-00079-7