Topic 4 Discussion 1

China is considered to have a highly functional cybersecurity division within its government, consisting of several organizations. Research and identify one of these organizations. Provide a brief description of the organization and a summary of your findings. Describe a recent attack where they have been caught performing malicious cyber acts. How has the government reacted? Finally, research and compare the U.S. cyber capabilities to those of China, providing a brief summary of your findings.

Hello Class,

China has a variety of organizations, including, The China Cyberspace Administration, a 2011- founded institution that reports to the Central Committee Information of China. This organization was responsible for internet content regulation and cyberspace security, which plays a significant role in organizing and overseeing online material. Independent actions carried out by the organization in China comply with Chinese law and the country's constitution. Moreover, the other Organization is The Ministry of Industry and Information of China. This 2008-founded body reports to the State Council and oversees the administration of Chinese manufacturing branches and the dissemination of industry information. This body is responsible for the ministry's industrial strategy, policies, and standards, as well as for keeping an eye on the day-to-day operations of the industrial branches.

Recently, there have been instances where China has been implicated in malicious cyber activities. One notable incident involved seven hackers associated with the Chinese government who were charged with computer intrusions targeting perceived critics of China and U.S. businesses. This attack highlighted the aggressive cyber tactics employed by certain entities linked to the Chinese government. In response to these cyber incidents, the Chinese government has maintained a stance of denying involvement in malicious cyber activities. Despite mounting evidence and accusations, the government has not publicly acknowledged or commented on specific attacks attributed to Chinese hackers. This lack of acknowledgment raises concerns about accountability and transparency in addressing cyber threats originating from within China.

When it comes to the US Government and the Republic of China Government our cybersecurity here in the United States are far proceeding of those of China. Currently the US is the only Tier 1 in cybersecurity in the world with China being close behind as the leading Tier 2 in cybersecurity. With the US making cybersecurity a priority since the 1990s is what has made the US get the Tier 1 category and the plan is to constantly stay on top as the only Tier 1 or the leading Tier 1 in cybersecurity in the world. The United States holds a position of clear superiority in cyber capabilities, but China is rapidly advancing and is expected to become a formidable competitor in the near future. Both countries are key players in the evolving landscape of cybersecurity.

References:

*China Cyber Threat Overview and Advisories | CISA*. (n.d.). Cybersecurity and Infrastructure Security Agency CISA. https://www.cisa.gov/china

*China Cybersecurity Companies*. (2018, September 18). Cybercrime Magazine. https://cybersecurityventures.com/china-cybersecurity-companies/

Washington, R. M. in S. F. and D. V. in. (2023, March 16). *WSJ News Exclusive | Wave of Stealthy China Cyberattacks Hits U.S., Private Networks, Google Says*. WSJ. https://www.wsj.com/articles/wave-of-stealthy-china-cyberattacks-hits-u-s-private-networks-google-says-2f98eaed

Williams, B. D. (2021, June 28). *US “Retains Clear Superiority” In Cyber; China Rising: IISS Study*. Breaking Defense. https://breakingdefense.com/2021/06/us-retains-clear-superiority-in-cyber-but-china-poised-to-challenge-study/