4-22-2022

Analysis of United States National Security Policy on Cyberterrorism from China

Megan Mead
Hope College

The Threat of Chinese Cyberterrorism In the United States

Megan Mead

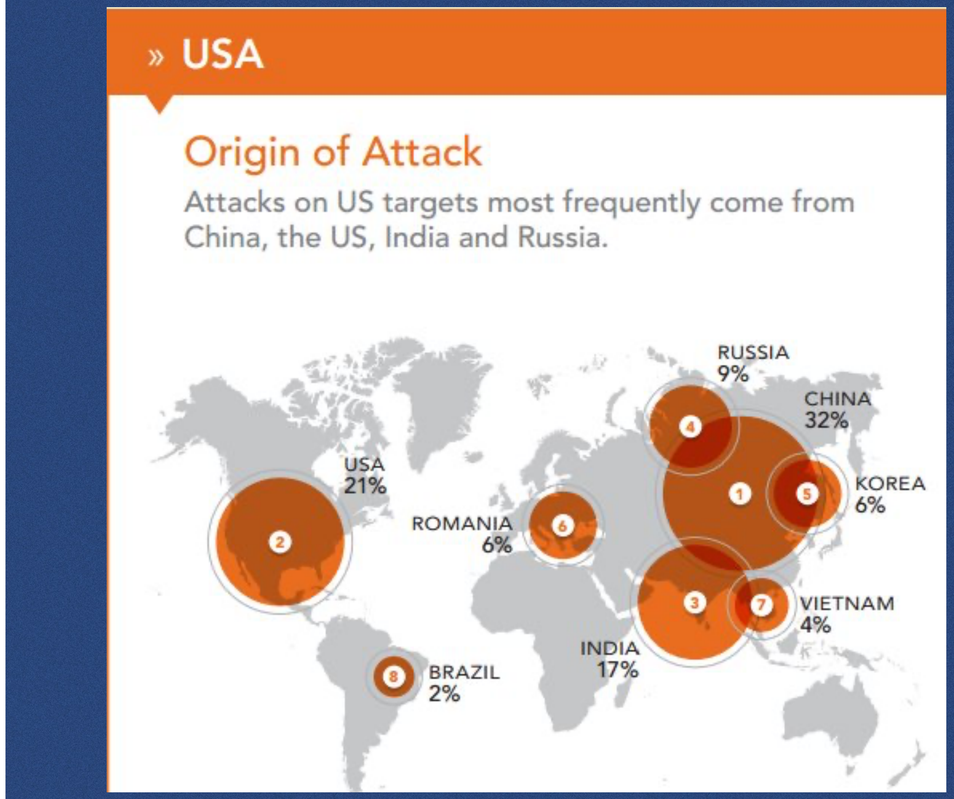
Are there credible threats and impacts on the United States' security and infrastructure due to Chinese cybertechnology?

Abstract

Cyberterrorism is a relatively new threat globally but has increased rapidly in recent years due to the development of more sophisticated and advanced technology. Many people question the existence of a substantial threat from the Chinese government in terms of their use of cyber technology on the United States. Intelligence shows China has continuously used their cyber capabilities as a way to exploit other countries, businesses, and local populations. Scholarly research, news outlets, and official government documents all conclude that Chinese cyberterrorism is a large security threat to the United States. China has used their technology to infiltrate U.S. networks and infrastructure in the past. This research examines the implications of how increased cyber attacks from China could be catastrophic to U.S. infrastructure, economy, and intelligence. Along with how the United States has combated previous attacks, developed new technology and implemented regulatory policy to protect infrastructure.

Policy Theories

- Punctuated Equilibrium Theory:
  - Long periods of stasis in the policy realm and a punctuating event occurs that opens up a window for rapid policy change.
- Policy Environments:
  - Political, economic, and social environments shape how people think and shape how policy is created and what policy is a priority.
- Bounded Rationality:
  - Limit on how much someone can know based on cognitive ability and knowledge. They make rational choices based on how much they have the ability to know.
  - In public policy administrators and policy makers are limited in their knowledge of the policy area, no one can never know all of the information, so it is important to recognize and accept that.



news.softpedia.com
2013 data

"More than 50% of attacks targeting the USA originated in China or Russia, with a further 27.8% of unknown origin"

"32% of China's attacks were directed at the USA, making the USA by far the biggest target for Chinese hackers"

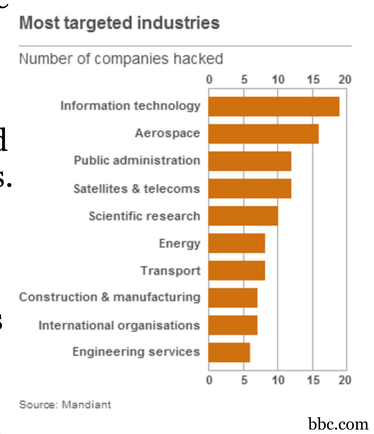
privacyaffairs.com
2009-2019 data

Take a picture to download the full paper

Full Final Draft

Analysis and Results

- China has become a large threat to U.S. national security in the cyber realm.
- Important industries and infrastructure are targets.
- Current policy and infrastructure is not protective enough.
- Academic policy theories can help explain the progression of cybersecurity policy thus far and enable improvement.



bbc.com
2013 data

Hacks primarily perpetrated by the Chinese government and Chinese firms

Policy Recommendations

- Proactive Policy:
  - Increased spending on infrastructure allows for the development of new technology in order to increase the safety of critical infrastructure.
  - Pursue a policy of deterrence instead of a protective strategy. This kind of strategy would utilize offensive measures in order to dissuade China from attacking due to fear of U.S. retaliation.

Selected Bibliography

Ad Ariely, Gil. "Adaptive Responses to Cyberterrorism." Edited by Tom Chen, Lee Jarvis, and Stuart Macdonald. Cyberterrorism, 2014, 175–95. https://doi.org/https://doi.org/10.1007/978-1-4939-0962-9_10.

Gould, Stephen Jay. Punctuated Equilibrium. Cambridge, MA: Harvard University Press, 2007.

Office of the Director of National Intelligence. Annual Threat Assessment of the US Intelligence Community. Washington DC, 2021. https://www.dni.gov/files/ODNI/documents/assessments/ATA-2021-Unclassified-Report.pdf

Klein, John J. "Deterring and Dissuading Cyberterrorism." Air and Space Power Journal: Afrique Et Francophonie 9 (2018): 21–34.

Simon, Herbert A. Models of Bounded Rationality : Empirically Grounded Economic Reason. 3. Vol. 3. Cambridge, MA: The MIT Press, 1997.