What is the future of cyber terrorism in the United states Government?

BY: Stephen Cobb

Cyber terrorism In the United States

- The United States Government is dealing with a big magnitude of cyber attacks from all parts of the world even on the homeland.
- The main Cyber attack threats come from Iran, Russia, China, and North Korea.
- The main struggle the US has right now is funding cyber defense strategies.
- Terrorism in general will strike fear into the nation as a whole and the government is what other countries will try to attack until they get it right.

Government strategies

- To beat these cybersecurity challenges agencies must produce new ways to protect their systems.
- The agencies that are doing the best right now with what they have are the ones who meet frequently to talk about strategies and review what is going on.
- Their strategies consists of Defending critical infrastructure, investing in a resilient future, and to make partners in the international level.

Federal Cybersecurity solutions

- Data Protection: This consists of things like end-to-end encryption, least-privilege access, and ways to track the movement of data.
- Network Security: Understanding what zero trust is in a network and using things like machine learning to detect threats early to manage attacks from spreading.
- Backups and Recovery: tools that can help an agency recover data quickly is important just in case of a ransomware attack. Like air-gapped backups.

Reasonings why cyber defense is so important on the federal level

- If the United States government prioritizes cybersecurity the level of cyberattacks would be less across the nation.
- Once cyber defense is important in our government all businesses will start to take it more seriously and understand what needs to be done in order to prevent cyber attacks and terrorism.

References

- CSIS, C. (2006). *Significant cyber incidents: Strategic technologies program*. https://www.csis.org/programs/strategic-technologies-program/significant-cyber-incidents
- Department, H. S. (2023, May 30). *Cybersecurity*. Cybersecurity | Homeland Security. https://www.dhs.gov/topics/cybersecurity
- Hua, J., & Bapna, S. (2012, December 8). *The economic impact of cyber terrorism*. The Journal of Strategic Information Systems. https://www.sciencedirect.com/science/article/abs/pii/S0963868712000522
- Kenney, M. (2014, December 18). *Cyber-terrorism in a post-stuxnet world*. Orbis. https://www.sciencedirect.com/science/article/abs/pii/S0030438714000787
- Shandler, R., Gross, M. L., Backhaus, S., & Canetti, D. (2021, February 10). *Cyber terrorism and public support for retaliation – A multi-country survey experiment: British Journal of Political Science*. Cambridge Core. https://www.cambridge.org/core/journals/british-journal-of-political-science/article/cyber-terrorism-and-public-support-for-retaliation-a-multicountry-survey-experiment/179C0560441076100DB4A4E5BBCB992F
- U, M. (2022, January 20). *Cyber terrorism: What it is and how it's evolved*. Maryville Online. https://online.maryville.edu/blog/cyber-terrorism/
- Weimann, G. (2004, December). *Cyberterrorism How Real Is the Threat?*. UNITED STATES INSTITUTE OF PEACE. https://www.usip.org/sites/default/files/sr119.pdf