

Open-source analysis of the cyber warfare capability of North Korea



Tyler Jensen and Dr. Samuel Liles

Abstract

This research provides an intelligence analysis, using information provided by publically-available sources, of the capability of North Korea to wage cyber war. Areas of closest consideration include infrastructure, past cyber attacks, availability of human actors to engage in cyber war, quality of education, and the quality of hardware and software available to the military. A close look at each area provides a big-picture look at the type and effect of future attacks that North Korea could use to engage in cyber war with the United States or its allies



Limiting Factors

- Poor educational system
- Lack of financial capital
- Few allies
- Aging telecom infrastructure

Enabling Factors

- Large pool of potential cyber warriors
- Little fear of attack attribution
- Extensive assistance from China
- Possibility of asymmetric advantage

Attributed Attacks

- Nonghyup bank shutdown
- S. Korean University graduate school hack
- DDoS on U.S. government websites
- Spear-phishing of S. Korean government employees

State-sponsored Actors

- Reconnaissance General Bureau (Unit 121)
- Mirim College
- State Security Agency
- Kim Chaek University

Conclusion

North Korea has made it very clear that they want to increase the size and capability of their cyber forces. Although they are a threat to the U.S., they lack the sophistication and funding of other threatening countries such as China and Iran. Their current attack capabilities are limited and will stay that way unless they make great strides in their educational system and computer hardware/software. The current cyber threat posed by North Korea is exaggerated by the South Korean government and media, which makes them seem more advanced than they really are. North Korea will continue to attack the United States and South Korea using cyber means but they don't currently possess the means to play on the same level as the U.S., Russia, China, and a few others.

