Was North Korea Behind the WannaCry Ransomware Attack?

Could the WannaCry ransomware attack have been perpetrated by hackers working on behalf of the North Korean government?

According to a security researcher for Google, the computer virus contained code in common with hacking tools previously used by the Lazarus Group. This is the hacking team that has been operating since at least 2009 that hacked into Sony Pictures in 2014.

That hack was in retaliation for the release of the motion picture *The Interview*, which was seen as an unflattering comedic portrayal of North Korean dictator Kim Jong-un. But, there are other connections that suggest the Lazarus Group is at least aligned with the Hermit Kingdom:

- in 2007, Operation Flame targeted the South Korean government for espionage, and may have been the hacking team's first attack;
- beginning in 2009, Operation Troy targeted the South Korean government for espionage;
- similar attacks to Operation Troy were conducted against the South Korean government in 2011 and 2013, code-named Operation 1Mission and DarkSeoul; and
- in 2016, the group attempted to steal $1 billion from the Bangladesh Bank, but was stopped after taking $81 million.

Internet security companies have been able to attribute cyberattacks based on patterns and code reusage. According to web security specialists, it's possible—but very unlikely—the code was added as a "false flag" to implicate Lazarus Group.

If the Lazarus Group was involved in the attack, and was working on behalf of the North Korean government, the next

question is how the U.S. and its allies will respond. Several Republicans have already called for Russia’s alleged meddling in the 2016 election to be declared an “act of war.”