



Press Release

FCC May Be Overstepping on Cybersecurity

PAULINA ENCK | FEBRUARY 4, 2025

Over the past two years, a hacking group linked to Chinese intelligence known as Salt Typhoon accessed U.S. telephone networks and systems used for court-appointed surveillance, collecting significant data on American users and government surveillance information. In a new insight, Director of Technology and Innovation Policy Jeffrey Westling reviews the Federal Communications Commission's (FCC) response to these attacks and considers the potential harms.

Key points:

- *Late last year, it was revealed that at least nine American telecommunications networks had been breached by Salt Typhoon.*
- *In an attempt to prevent future attacks, the FCC broadly interpreted its authority over telephone networks and some broadband internet service providers to include the regulation of cybersecurity practices, and could extend these regulations to other forms of communication such as broadcast television or satellite broadband.*
- *While defending American networks from Chinese cyberattacks is a key federal priority, drastically expanding the FCC's authority without congressional approval could hinder any whole-of-government approach to secure American networks and unintentionally make those networks less secure by deterring collaboration between industry and federal regulators.*

[Read the analysis](#)