

THREE MODELS OF STATE CONTROL OVER CYBERCRIMINAL PROXIES: EVIDENCE FROM RANSOMWARE OPERATIONS



April 1 at 4:30 - 6 p.m.
DMC Theater, LSU Digital Media Center

Karen Nershi

MIDDLEBURY INSTITUTE OF
INTERNATIONAL STUDIES

ABSTRACT

States increasingly employ cybercriminal proxies to conduct covert operations while maintaining plausible deniability, but empirical evidence about the nature and extent of state control remains limited. I develop a revealed-preference approach using operational timing patterns to detect and distinguish different models of state-cybercriminal relationships. Analyzing 13,250 ransomware attacks across 17 countries from 2020-2025, I identify three distinct operational models. First, Russian-linked groups show a reduction in activity during Russian holidays, consistent with semi-autonomous operations in which the state provides safe haven to criminals who retain operational independence. Second, North Korean-linked operations show a decrease in activity on Kim family birthdays and primarily target South Korean victims, consistent with state-directed operations that serve strategic state objectives. Third, an Iranian-linked group began attacks days after a major escalation in Iran-Israel tensions and sustained operations through religious holidays while targeting primarily Israeli victims, consistent with conflict-mobilized cyber warfare. These findings provide compelling empirical evidence of varying state-criminal models of operation and introduce a generalizable method for detecting state influence over non-state actors. The results have important implications for understanding how states employ cybercriminal proxies during both peace and conflict.

SPEAKER BIO

Karen Nershi is an Assistant Professor of Cybersecurity and Co-director of the Cyber Collaborative at the Middlebury Institute of International Studies. Through an empirical lens, her research examines international security and cooperation challenges in cybersecurity. Specific topics her research explores include ransomware and money laundering risks in the cryptocurrency sector. Her peer-reviewed research has been published in Political Science Research and Methods and the Journal of Cybersecurity. Before joining MIIS, Nershi was an Assistant Professor at IE University in Madrid, Spain and a Postdoctoral Fellow at Stanford University's Stanford Internet Observatory. She completed her Ph.D. in political science at the University of Pennsylvania in 2021.