Abstract

Cyber threats regarding China's political espionage and intellectual property theft have featured prominently in United States (U.S.) government's public discourse in recent years. This thesis examines the threats that China's cyber-attacks pose to U.S. national security and critically assesses whether the government discourse surrounding China's cyber-attacks accurately reflects the actual threats. Overall, the study shows that China's cyber-attacks do not pose an existential threat to U.S. national security, contrasting U.S. government officials' claims which tend to exaggerate and depict Chinese cyber-attacks as an existential threat. Based on cyber-attack data between the U.S. and China from January 2013 to May 2019, this paper observes that China primarily conducts long-term espionage, exerting economic, diplomatic and social impacts, but does not conduct any degradative cyber-attacks. The study also observes from government statements surrounding two cyber-attacks – Office of Personnel Management (OPM) hack and Operation Cloudhopper – that U.S. government officials exaggerated China's cyber-attacks in imposing counterintelligence impacts of mortal danger, and inflated China as an unprecedented threat that unfairly benefits Chinese firms at the expense of U.S. firms. This paper concludes that Chinese cyber-enabled political espionage poses intelligence and counterintelligence effects that affect U.S. national security. However, these effects do not constitute an existential threat to U.S. national security, unlike what U.S. government officials have claimed. The U.S. understands and responds to China's cyber-attacks, and thus poses an equal, if not greater, threat to China. This paper also asserts that cyber-enabled commercial espionage impacts U.S. national security via economic consequences, but it forms a small part of the broader systemic threat underlying China's other forms of legal and covert transfer of technology. The Chinese government's direct involvement in commercial espionage against U.S. firms may be exaggerated given the personal commercial incentives of private firms to unilaterally conduct commercial espionage. Overall, U.S. government officials' accusations of China are weakened by similar cyberespionage activities that U.S. intelligence agencies conduct, the refusal or inability of the U.S. government to provide the public with direct evidence, and the muddling of national security issues with trade goals.