Deterring the Impossible: An Analysis of Successful Cumulative Deterrence Within Cyber Space Between the United States and Russia

by Elizabeth M. Flatoff

Deterrence theory has been successfully applied to a nuclear age, but has been struggling to keep up with the ever-evolving world of cybersecurity. Perfect deterrence theory hinges on two major aspects, credibility and capability; depending heavily on the rational choice theory and the idea that humans make rational choices and weigh pros and cons before acting -- especially on an international scale. But the lack of accountability and incentive for actors to claim responsibility for any sort of cyberattack, means one major aspect of perfect deterrence is missing-capability. If states lack the capability to determine who started or undertook the attack, they cannot respond nor deter effectively. For this reason, the debate around cyber deterrence is changing; rather than perfect or general deterrence, cumulative deterrence is beginning to be applied to case studies around cybersecurity. While it was first applied to Israel and their nuclear deterrence policy, this paper aims to apply the framework to the cyberspace between the United States and Russia. Due to similarities in capabilities and power between the United States and Russia, the United States is able to use cumulative deterrence more successfully against larger Russian cyberattacks -- smaller attacks that cannot yield any repercussions are harder to deter. The cumulative deterrence framework explores the importance of allies, modern technology, creation of new strategies and conditions, and past victories. While analyzing these variables this paper will explore the extent in which the United States can successfully deter Russian cyberattacks.