

## **Borders in Cyberspace: Can Sovereignty Adapt to the Cyber Security Challenge?**

Forrest Hare

George Mason University

The new United States (US) administration has begun efforts to securitize the substantial problems the United States is currently facing in cyberspace. Recently, President Obama ordered his National Security Council to conduct a rapid review of existing measures being undertaken by the federal government, and provide recommendations for additional ones. He also promised to appoint a national advisor for cyber security issues. Many stakeholders in the US government and private industry are watching these actions closely as there seems to be broad acceptance that the issues call for more extensive security measures. However, effective securitization of threats in cyberspace will be complicated by many issues. First the nature of “cyber security” as a national security issue is ambiguous. Not all stakeholders agree on the priorities or where the focus of security measures should be. Second, there is a potential for a security dilemma. Efforts by the US government, or any state actor, to increase cyber security through sovereign measures, especially since such measures would be difficult for others to monitor, could be seen as attempts to militarize the domain. And lastly, due to the inherent inter-connectedness in the domain, cyber security is a “trans-sovereign” issue affecting both developed and developing countries in an interdependent manner.

There is considerable debate as to whether the concept of borders is relevant to the challenges of cyber security, because actors in cyberspace enjoy relative anonymity and can threaten inter-connected targets around the globe. The discussion is often conflated with the issues of privacy and commerce across the Internet. Regardless the focus, the concept of borders is important because they define the territory in which national governments can employ sovereign measures. To analyze borders in the context of cyber security, this paper asks the question, “Is there an important role for the concept of borders, if not physical lines, in improving national security in cyberspace?” To explore the question, I will take two approaches. First, I will conduct a comparison of the cyber security issues to international drug-trafficking. In doing so, I will explore ways in which the problems may be comparable. If they are comparable, I will discuss sovereign measures used to combat drug trafficking that may be applicable to improving cyber security. The second approach is an examination of the issue from the perspective of the Heil and Kunreuther Inter-Dependent Security Model. Can the IDS model be applied to the national-level cyber security problem? If so, will it inform the cyber security decision process of national governments as they consider options to invest in a higher level of security?

The paper will argue that, whether the problem is addressed from the stand-point of criminal behavior like drug-trafficking, or cyber attacks in an interdependent, global domain, borders can be a potentially useful construct to address cyber security issues and inform national policy decisions, regardless of the physical location of relevant nodes. However, sovereign powers must be careful not to use the concepts of borders to curtail the progress our nations have made to connect and better the world via this evolving and expanding environment. In other words, we can no more lock down the borders to counter malicious actors in cyberspace than we can lock down our nation’s physical borders to fight terrorists and drug-traffickers.