



HOKKAIDO UNIVERSITY

Title	サイバー空間と国家主権
Author(s)	塩原, 俊彦
Citation	境界研究, 5, 29-56
Issue Date	2015-03-04
DOI	https://doi.org/10.14943/jbr.5.29
Doc URL	https://hdl.handle.net/2115/61163
Type	departmental bulletin paper
File Information	02Shiobara_10Summary.pdf, 英文要旨



Cyberspace and State Sovereignty

SHIOBARA Toshihiko

The concept of cyberspace is only a metaphor, as well as telegraphy. On the one hand, those who believe in the absence of territorial borders in cyberspace can insist that state sovereignty has nothing to do with cyberspace. On the other hand, the argument that cyberspace should be defined as a global domain within the information environment consisting of the interdependent networks of information technology infrastructures and resident data has gained in power recently. Because of the fact that infrastructures are located in some territories, the state can lay claim to jurisdiction over cyberspace.

In order to investigate the appropriateness of the insistence of the state, we explore how the state gains jurisdiction over land, sea, air, and space historically. Although modernization enabled the state sovereignty to govern some territories through international laws, this does not mean that such control of the state is universal. Never forget that the state is only a *deus mortalis*, that is, a “mortal God,” as Thomas Hobbs wrote in *Leviathan*.

In the National Defense Strategy of the United States of America published in 2005, it is stated that the ability to operate in and from the global commons—space, international waters and airspace, and cyberspace—is important. Nonetheless, the US government changed its position that the global commons include cyberspace after Barack Obama was elected president of the United States. The US government had begun to insist that each state could insist on jurisdiction over cyberspace, because cyberspace consisted of information infrastructures and data. It encouraged experts to make so called *Tallinn Manual*. Tallinn Manual applicable to cyber warfare will become the basis of the international law on “cyber war.”

Nevertheless, we cannot authorize this “realistic approach.” This approach is only an opinion of the United States, losing hegemony in the world. Although the hegemon tries to have an influence on experts through the cyber-industrial complex, we can criticize the modus operandi of the United States. We can propose an “idealistic approach” based upon the absence of territorial borders in cyberspace.