

Sovereignty 2.0 - digital sovereignty in light of international law

Traditional definitions employed by international courts and scholars construe sovereignty as “the right to exercise [in regard to a portion of the globe], to the exclusion of any other State, the functions of a State.” This exclusivity of authority is challenged in cyberspace for two reasons: first, due to the interconnectedness of cyberspace States increasingly exercise their power and authority over data and internet infrastructure located on the territory of other States. Second, to properly exercise their functions in the digital environment, States may have to rely on Internet infrastructure located within other States (and thus subject to their jurisdiction) and governed according to rules over which they have no say. This has led to the emergence of a novel concept of “digital sovereignty”, by which States such as France, Germany, China and Russia, but also the European Union, seek to achieve the preservation of core tenets of sovereignty, especially the exclusivity of State authority, in the technical realities of cyberspace.

The proposed research project aims at reappraising the role and function of the principle of sovereignty in the digital environment. By assessing the normative content and scope of the emerging concept of “digital sovereignty”, the project pursues the question whether digital sovereignty forms an answer to the challenges to State authority, posed by a globally interconnected medium such as cyberspace and how it fits with the public international law principle of sovereignty.

To this end, it will pursue the following research questions:

1. What is the normative content of the concept of “digital sovereignty”?
2. Are the interpretations of this concept presented by States mutually exclusive, complementary or overlapping?
3. How does “digital sovereignty” address the constituent elements of “traditional” sovereignty – exclusive authority over a given territory?
4. How does “digital sovereignty” influence (expand? curtail?) the traditional public international principle of sovereignty.

The questions lead to two working hypotheses, which will be tested during the research: first, that “digital sovereignty” is more than a political buzzword and has normative content to the extent that it comprises the regulatory power of the State in the digital realm and the State’s strategic autonomy, i.e. the ability to act in the digital sphere without being restricted by external dependencies. Second, that these aspects are reconcilable with a “Westphalian” definition of sovereignty, but will lead to a readjustment of exclusive State competences towards shared authority/jurisdiction in certain areas (shared internet governance, legality of low-intensity cyber operations).

The project has a multi-faceted structure, which impacts the shape of the research plan. The research plan consists of three major steps. In the first phase, the Principal Investigator, with the help of a research team, will research and collect digital sovereignty – related laws and policies of five major States (China, France, Germany, Russia and the United States) and one Int. Organisation (European Union). The research will concentrate on four main issues: territorial sovereignty, data sovereignty, Internet governance and autonomy in regulating national internet infrastructure. In the second phase, the PI will assess the normative content of each State’s concept of digital sovereignty, to establish common denominators as well as differences in interpretation. In the last step, the PI will assess how the analysed digital sovereignty-related practice of these States will influence (or already influences) the content and scope of the general principle of sovereignty in international law. Finally, the PI will formulate conclusions with the aim of establishing what a “digitally sovereign” State looks like.

The project’s novelty and importance lie in a synthetic approach to the highlighted issue, which will result in a general theory of sovereignty in cyberspace, and an inclusion of non-Western (Chinese, Russian) source material, which will give a broader international outlook and help integrate non-Western arguments into the Western legal discourse.

The project will result in a comprehensive and multi-faceted overview of most recent State practice relating to the concept of digital sovereignty from major cyber powers and the formulation of a general theory of sovereignty in cyberspace. Partial results of the research will be published in articles and full conclusions in a monograph summing up the findings of the project.