Abstract

This thesis deals with the complex issue of cyber security in international relations, specifics of cyber realm due to its technical nature and particular circumstances of its development as well as with the way how the EU deals with information and communication technologies. Even though cyber security as a category appears with increasing frequency and intensity in the thinking on security and related political debate in the past twenty years, some of its basic tenets are still insufficiently understood. First part of the thesis deals with cyber realm and its specifics as such with effort to pinpoint some of the inherent contradictions between the traditional Westphalian nation states and the fluid character of the digital world. Through analysis of selected relevant incidents as well convincing absence of the "digital-doom" scenarios the peculiar expectation-reality discrepancy will be analysed. The overarching method departs from intersubjective securitization framework. In the last part analysing the EU it is the concept of *threat framing* that is applied to study and trace the narrative of the EU in these matters. Here a gradual construction of a narrative termed ICT as "fundamental societal building block" reveals itself with cyber related issues making its way into top policy levels through various channels: Cyber-crime, Cyber-defense, Critical Infrastructure Protection, Counter-Terrorism and overarching normative effort termed Digital Agenda.