

## **Abstract**

This thesis presents a comparison of the cybersecurity strategies of the United States and the United Kingdom. The more advanced a society is, the more it tends to be digitised and dependent the security of cyberspace. Due to this dependence, states are extremely vulnerable to internal or external cyber attacks and assaults on their information systems. This creates entirely new vulnerabilities, both for states as such and for society as a whole. This thesis presents and compares the institutional response mechanisms of both states in the event of a cyber incident. These mechanisms are approached against the backdrop of the historical development of cyber strategies as well as demonstrated through selected cyber incidents. Both the United States and the United Kingdom use the cyber deterrence method as their main mechanism for dealing with cyber threats, which was also used in the aforementioned attacks. This thesis aims to present the effectiveness of this strategy and place it in the context of cyber security strategy as a whole. It shows that although the cyber deterrence approach should be an integral part of every state's cybersecurity strategy, it would be advisable to pay increased attention to other approaches as well as to the preparation of offensive cyber strategies.