ABSTRACT

This thesis is an attempt to analyse the relationship between the increasingly popular concept of national resilience and cybersecurity. National resilience is a concept that has permeated the security and policy making realms in recent times. This relationship is examined by using the Baltic nation of Estonia as a model due to the nation being regarded as the 'most digitally advanced in the world'. The main objective of the thesis is to investigate the relationship between cybersecurity and national resilience and discuss the implications of this relationship in the wider security context. The thesis begins by establishing if a nexus exists between the concept of national resilience and cybersecurity. In order to better understand the potential impact cyber security could have on a nation's resilience, it is important to establish the relationship between the two concepts. After the nexus is successfully established, the thesis then charts the development of the concept of resilience within the Estonian national security documents. The aim of this exercise is to demonstrate how the concept of resilience has been transformed over the years within an Estonian context while comparing its trajectory to the wider global trend of the concept. The research technique of content analysis is utilised to systematically examine the national security documents of Estonia.

After the concept of resilience is contextualised in case of Estonia, the thesis will endeavor to explore how cybersecurity and national resilience interact on a practical level. The protection of Critical Infrastructure is considered one of the fundamental components of maintaining the resiliency of a nation. In 2018, the fact that National Critical Infrastructure is increasingly reliant on digital systems for operability of its systems was recognised. Thus, cybersecurity plays a key role in protecting these systems from malicious actors in vital sectors such as the energy sector, state agencies, the transport system and the financial sector. This section of the thesis will utilise case studies in the form of the Estonian energy sector and its state agencies to demonstrate the importance of the cybersecurity, i.e. the national resilience nexus.

The final chapter attempts to explain how a healthy civil society tradition can help improve the national resilience building capacities of a nation. This chapter will have a particular focus on the cybersecurity sector as Estonia appears unique in so far as the fact that it possesses volunteer organisations specifically dedicated to defending Estonian cyberspace. This chapter will draw on Estonia's long history of inter-agency cooperation to demonstrate how civic responsibility can be utilised to bolster a nation's resilience.

The findings of this research project will be tied together in a concluding section which aims to explain the effect that cybersecurity has on national resilience and what the results from the Estonia case demonstrate in the wider context.