Since the start of the Ukraine war Ukraine has experienced a threefold increase of cyber-attacks from Russia. Ukraine, the United States, Germany, and France have already experienced continuous cyber-attacks from Russia since 2014. Although the National Cyber Security Strategies (NCSSs) from the latter three have already been compared amongst each other and others in academic literature, the NCSS of Ukraine has not. No NCSS has also been analysed for resiliency against the Russian cyber doctrine. The main research question answered was: what can states and organisations learn from the NCSS of Ukraine, compared to the United States, Germany and France assessed on their resiliency against the Russian cyber-attack doctrine since 2014? The question was answered with the help of three research questions. The first aimed to analyse the Russian cyber doctrine before and after the start of the war and develop a framework with the most common targets and Tactics, Techniques and Procedures (TTPs) with which NCSSs can be compared against each other on scores based on their resilience. The most common targets have been those of critical infrastructure sectors and TTPs being DDoS, phishing, and ransomware. The second research question aimed to see which NCSS was most resilient, which was the one of Ukraine. This was due to its recent strategic initiatives it implemented to defend itself. The third research question aimed to give recommendations based on the comparison. The answer to the main research question is based on the recommendations that states and organizations can learn from regarding their cyber security strategy which is to give attention to the most common used TTPs and implement a holistic approach to cyber security to defend against them.