Abstract: Criminals and other threat actors are adapting to the growing reliance individuals, organisations, and nations have upon technology and the internet and have augmented their capabilities to be oriented in that direction for malevolent purposes. Cyberspace has become an extremely large vulnerability for countries because it facilitates any person with access to a computer or other technology along with malicious intent, to cause harm. The increased risk people and organisations now face in cyberspace is not isolated to just them. Nations now are also at an increased risk because of the evolving ubiquity of cyberspace and technology. States are at risk of cyber threats because of vulnerabilities in individual citizens and organisations. Nations have now become intended targets by a larger spectrum of threat actors. This research examines how the United Kingdom has developed their specific national cyber security strategy to improve national resilience to threats, and how well the UK government adapts to an ever-changing threat landscape. The UK is still deficient in the appropriate and thorough execution of their proposed strategies and strategic policies to attain national resilience and security. There have been strides to achieve that goal, but the national strategy continues to fail to contextualise past cyber-attacks and input those lessons into practice. Until the UK can develop and implement strategy that is up-to-date with the current trends in cyber threats at a quicker pace, they will not be able to maintain resilience or security in cyberspace.