Abstract

The present thesis deals with the US strategic approach and posture to cybersecurity from a national point of view. On such a topic much has been written already, nonetheless the present work finds a degree of originality by tackling such object of analysis shifting the focus to a ideational perspective. By drawing insights from the meta-theory of Constructivism and the rich research tradition on strategic culture, the present thesis aims at understanding what kind of norms seem to be informing/mirroring what has been labelled the US "cyber strategic culture", and if it is possible to speak of a "shift", or at least track an evolution regarding them, in a historical timeframe that runs from the early 2000s up to the present days. To pursue the stated research agenda, a methodology grounded in discourse and thematic analysis is utilised, with an analytical framework centred around two opposite "thematic normative categories" (themes) called "defensiveness" and "offensiveness", each characterised by a "story" made up by three sub-themes, delineating specific strategic behaviours. A set of official strategies, all tackling cybersecurity and published during the mentioned timeframe by both the White House and the military, form the primary sources to which such methodology is applied, with particular focus being posed to the defensive paradigm known as "active cyber defence" measures, the 2015 Department of Defense's Cyber Strategy, and the 2017 National Security Strategy. Overall, it is argued that, despite a predominant presence of the theme of "defensiveness", it is indeed possible to speak of an on-going evolution, especially since 2011, which sees the norm of "offensiveness" increasingly informing the US "cyber strategic culture".