Chapter 5
Building Blocks and Measurement of National Cyberpower

Joey Jansen van Vuuren
Tshwane University of Technology, South Africa

Louise Leenen
University of the Western Cape, South Africa

ABSTRACT

Cyberspace and cyber threats are increasingly recognized to pose a significant risk to a state's security. Cyberpower is central to national power and thus a driver towards the attainment of national security. The authors decompose national cyberpower by analyzing the elements of cyberspace as part of national security. David Jablonsky distinguishes between natural and social determinants of power in his discussion of national power and refers to Ray Cline's formula to determine a rough estimate of "perceived" national power by focusing primarily on a state's capacity to wage war. The authors present an adaptation of the formula for perceived power for use in cyberspace to create a similar formula for perceived cyberpower that focuses primarily on a state's capacity for cyberwarfare. Military cyberpower is one of the critical elements of cyberpower but little attention has been paid to this concept in the literature. In this chapter, concepts such as cyber effectiveness and the operationalization of military cyberpower are also addressed.

DOI: 10.4018/978-1-5225-8304-2.ch005

INTRODUCTION

… there is a relationship between the ability of a state to effectively employ military power (or combat power) and victory. Effectively employing cyber power may mean the difference between winning and losing modern battles (Bebber 2017).

A state's national power comprises of several elements, one of which is cyberpower. Cyberpower is defined as the strategic employment of information and communication technologies to enable economic growth, empower society and enhance security (McConnell, 2012). The relationship between 'cyberpower' and 'national power' can only be investigated if there is a common understanding of both national terms. National power has been explored extensively in academic literature, but cyberpower and its relationship with national power needs more analysis. Therefore, this chapter consists of interlinked parts that provides a discussion on the main issues concerning the building blocks in measuring national cyberpower. A discussion on national security, including national power, is conducted in Section 2. Section 3 takes a closer look at Cyberpower, arguing that cyberpower is not limited to only military power. The authors use Kern (2015) and Young (2010) to discuss the absence of a theory or doctrine for the operationalisation of military cyberpower. Taking this into consideration, Section 4 gives an overview of principles that have been formulated in this regard. In Section 5, the discussion moves to a perception of cyberpower as a part of national power. The authors argue that the initial conceptualisation of cyberpower as either an independent attribute or an element of an existing attribute of national power, is insufficient. It is largely because later conceptualisation conceded that cyberspace has both its foundations and utility in all the attributes of national power. The authors also posit that cyberpower is both physical attributes and an abstraction or synergy of all these attributes. Therefore, cyberpower is best understood as a way of achieving national power, rather than simply as a means or attribute of national power. An argument is also made that cyber effectiveness is a translation of cyberpower through technical, tactical, operational and strategic means (Bebber, 2017). The next step is an analysis of national power formulas (Section 6). The formulation of national power, as proposed by Cline (1993), is used as a starting point to develop a perceived cyberpower formula. This chapter concludes with the development of a formulation for perceived cyberpower (PCP). The latter is expressed as replication or fractal of national power, and not as a unique independent attribute (Section 7).[1]