International Journal of Cyber Warfare and Terrorism
Volume 7 • Issue 3 • July-September 2017

Formulating the Building Blocks for National Cyberpower

JC Jansen van Vuuren, University of Venda, Thohoyandou, South Africa & CSR Defence, Peace, Safety and Security, Pretoria, South Africa

Louise Leenen, CSIR Defence, Peace, Safety and Security, Pretoria, South Africa

Graeme Plint, Department of Defense, Pretoria, South Africa

Jannie Zaaiman, Belgium Campus, Pretoria, South Africa

Jackie Phahlamohlaka, CSIR Defence, Peace, Safety and Security: CSIR, Pretoria, South Africa

ABSTRACT

Cyber threats pose a growing risk to national security for all nations; cyberpower is consequently becoming an increasingly prominent driver in the attainment of national security for any state. This paper investigates the national cyberpower environment by analysing the elements of cyberspace as part of national security. David Jablonsky (1997) distinguishes between natural and social determinants of power in his discussion of national power. Also, Jablonsky refers to Ray Cline's formula (Cline, 1993) to determine a rough estimate of "perceived" national power by focusing primarily on a state's capacity to wage war. In this paper, the formula for Perceived Power (PP) will be adapted for use in cyberspace to create a similar formula for Perceived Cyberpower (PCP) that focuses primarily on a state's capacity for cyberwarfare. Military cyberpower is one of the critical elements of cyberpower. The paper also discusses how to operationalise military cyberpower.

KEYWORDS

Cyber Defense, Cyberpower, National Power, National Security

INTRODUCTION

To investigate cyberpower's relationship with national power, a common understanding of national power and its formulation is required. This paper starts with a discussion on national security (Section 2), national power (Section 2.a) and cyberpower (Section 3) that is not limited to military power alone. Kern (2015) and other authors (Young, 2010) discuss the absence of a theory or doctrine for the operationalisation of military cyberpower. Section 3.1 gives an overview of principles that have been formulated in this regard.

The discussion then moves to a perception of cyberpower as a part of national power in Section 4. It is argued 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

DOI: 10.4018/IJCWT.2017070102

Copyright © 2017, IGI Global. Copying or distributing in print or electronic forms without written permission of IGI Global is prohibited.

conceptualisation conceded that cyberspace had both its foundations and utility in all the attributes of national power. It is also argued 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.

The next step is an analysis of national power formulas (Section 5). The formulation of national power proposed by (Cline, 1993) is used as a starting point to develop a perceived cyberpower formula. The paper concludes with the development of a formulation for perceived cyberpower (PCP) that is expressed as replication or fractal of national power, and not as a unique independent attribute (Section 6).

NATIONAL SECURITY

National governments have the responsibility to provide, regulate and maintain national security, which includes cybersecurity or human security to their citizens (Jablonsky, 2001). David Jablonsky (2001) defines national security as that part of government policy with the objective to create national and international political conditions favourable for the protection, or the extension of vital national values, against existing or potential adversaries. He extends this definition by adding the respective elements of the power base of the state and the priorities that are seen as of important and/or national interest. Jablonsky's (2001) description of the concept of national security regarding the elements of national power can be regarded as a significant contribution to national security theory, even though there are as many definitions of the concept as there are scholars of national security. For this reason, the definition of national security as formulated by (Phahlamohlaka, 2008) is adopted: "The provision of security to the state and of human security to its citizens as well as the protection of national and human interests together with state borders through the projection of national power".

National Power

With the intention to exploit "cyberspace" for the attainment of national power, there is a pressing need to investigate the relationship between cyberpower and national power. Although this relation may seem self-evident, the way cyberpower is conceptualised in relationship to national power will have a severe impact on the strategies, organisations and structures that will emerge from the national security strategy.

National power consists of various elements, also called instruments or attributes that can be grouped together according to the origin. These groups include geography, population, military and economy (Jablonsky, 1997, 2001, 2010). Furthermore, Jablonsky (1997) indicates that power is a relative attribute that is contextual in nature and entails a synergy of state activities. National power thus cannot be studied or understood in isolation from the desired outcomes, context as well as relative strengths and weaknesses of the nation. Also, Jablonsky (2001) asserts that the elements of power cannot be easily quantified and if this is attempted the measures could be contradictory in nature. These elements are defined in terms of natural and social determinants of national power. The natural determinants (geography, resources, and population) are concerned with the number of people in a nation and with their physical environment. Social determinants (political, informational, military, economic and psychological) on the other hand, concern the ways in which the people of a nation organise themselves and the manner in which they alter their environment. Jablonsky (2001) thus inadvertently provides the foundation for the acronym DIME (Diplomacy, Information, Military Economics). Jablonsky (2001) also refers to a formula introduced by Cline (1993) which provides a rough estimate of "perceived" national power that focuses primarily on a state's capacity to wage war.

11 more pages are available in the full version of this document, which may be purchased using the "Add to Cart" button on the publisher's webpage: www.igi-global.com/article/formulating-the-building-blocks-for-national-cyberpower/185601

Related Content

SQL Code Poisoning: The Most Prevalent Technique for Attacking Web Powered Databases
Theodoros Tzouramanis (2007). *Cyber Warfare and Cyber Terrorism (pp. 161-171).*
www.irma-international.org/chapter/sql-code-poisoning/7453

A Learning-based Neural Network Model for the Detection and Classification of SQL Injection Attacks
Naghmeh Moradpoor Sheykhkanloo (2017). *International Journal of Cyber Warfare and Terrorism (pp. 16-41).*
www.irma-international.org/article/a-learning-based-neural-network-model-for-the-detection-and-classification-of-sql-injection-attacks/181791

Good Governance and Virtue in South Africa's Cyber Security Policy Implementation
Oliver Burmeister, Jackie Phahlamohlakaand Yeslam Al-Saggaf (2015). *International Journal of Cyber Warfare and Terrorism (pp. 19-29).*
www.irma-international.org/article/good-governance-and-virtue-in-south-africas-cyber-security-policy-implementation/135271

Denial-of-Service (DoS) Attacks: Prevention, Intrusion Detection, and Mitigation
Georg Disterer, Ame Allesand Axel Hervatin (2007). *Cyber Warfare and Cyber Terrorism (pp. 262-272).*
www.irma-international.org/chapter/denial-service-dos-attacks/7463

Modeling and Simulating Student Protests Through Agent-Based Framework
Tshepo Solomon Raphiri, Joey J. Jansen van Vuurenand Albertus A. K. Buitendag (2023). *International Journal of Cyber Warfare and Terrorism (pp. 1-20).*
www.irma-international.org/article/modeling-and-simulating-student-protests-through-agent-based-framework/319708