Building blocks for National Cyberpower

JC Jansen van Vuuren[1,3], Graeme Plint[2], Louise Leenen[1,3], Jannie Zaaiman[3], Armstrong Kadyamatimba[3], J Phahlahmohlaka[1]

[1] Defence Peace Safety and Security: CSIR, Pretoria, South Africa
[2] Department of Defence, Pretoria, South Africa
[3] University of Venda, Thoyandou, South Africa
jjvvuuren@csir.co.za
gw.plint@di.mil.za
lleenen@csir.co.za
Jannie.zaaiman@univen.co.za
armstrong.kadyamatimba@univen.co.za
jphahlamohlaka@csir.co.za

Keywords:. Cyberpower, National Power, National Security, Cyber Defence,

Abstract:
With the advancement of technology and proliferation of mobile and computing devices through all levels of society, cyber power is becoming an increasingly prominent driver in the attainment of national security for any state. This paper investigates the national cyberpower environment by analyzing the elements of cyberspace as part of national security. To understand cyberpower as a contributor to national security, one must identify and analyze the elements of national cyberpower and how they interrelate to national power.

In his discussion on national power, David Jablonsky (Jablonsky, 1997) distinguishes between natural and social determinants of power. In addition, Jablonsky refers to the Ray Cline's formula (Cline, 1993) to determine a rough estimate of "perceived" national power by focussing primarily on a state's capacity to wage war (Jablonsky, 1997). The problem posed is how cyberpower can be best positioned within Jablonsky's proposed model for national power and the formula of Cline. 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) in context that will primarily focus on a state's capacity for cyberwarfare.

1. Introduction

In investigating cyberpower's relationship with national power, a common understanding of national power and its formulation is required. The formulation of national power proposed by Cline (1993) will be used as a starting point. However, a few caveats need to be registered; firstly the pseudo-mathematic formulation of the "formula" must be seen as a theoretic formulation and not a quantifiable formula. This concession must be made in the face of both Jablonski's critique as well as the findings of the RAND corporation (Jablonsky, 2010; Treverton & Jones, 2005). Secondly, the understanding of the attributes of power has been successfully conceptualized beyond Cline's argument of critical mass, economics and military, and presently include diplomatic, informational, military, economic and others (Steele, 2006). DIME (diplomacy, information, military and economics) is a military term to remind the leadership and policy makers above them to consider national power as not limited to the military power alone (Shehadey, 2013).

This paper acknowledges that cyberpower is a multifaceted phenomenon. Kuehl points out that there are three distinct layers of cyberspace and thus cyberpower, namely the physical, then informational and lastly the cognitive (Kuehl, 2009). This presentation neatly dovetails with the argument presented in this paper. The argument is simply that for cyberpower to be seen in relation to national power (in accordance with the Cline (1993) formula) it needs to be reconciled to both the physical attributes (as represented by DIME) as well as the cognitive levels of abstraction that are included in the "Strategic purpose and National Will" or intangible part of the formula.

This article will argue that the initial conceptualization of cyber power as either an independent attribute or an element of an existing attribute of national power is insufficient. This is largely because later conceptualization 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 and is thus cyber power is best understood more as a way of achieving national power, than simply a means or attribute of national power. Thus, for a formulation for perceived cyberpower (PCP) would be best expressed as a replication or fractal of national power, and not a unique independent attribute.

National security, national power and cyberpower are discussed in the following three sections: 2, 3 and 4 where cyberpower is considered as a part of a nation's power. In Section 5 cyberpower as a part of national power is discussed, and in Section 6~~5~~ formulas for national power are investigated. Based on the previous sections' results, Section 7 presents a formula for cyberpower. The paper is concluded in Section 8 with the development of a perceived cyberpower formula.

2. 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 to 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 vital and/or national interest. Jablonsky's (2001) description of the concept of national security in terms of the elements of national power could be regarded as a major contribution to national security theory, even though are as many definitions of the concept as there are scholars of national security. For this reason, we adopt in this paper the definition of national security as formulated by (Phahlamohlaka, 2008) who defines national security as: "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".

3. National power

With the intent to exploit "cyberspace" for the attainment of national power, there is an increased need to investigate the relationship of "cyberpower" and national power. Although this relationship may seem self-evident, the way cyberpower is conceptualized in relationship to national power will have a serious impact on the strategies, organizations 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 origin. These groups include geography, population, military and economy (Jablonsky, 1997). 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 and relative strengths and weaknesses of the nation. In addition, Jablonsky indicates that the elements of power cannot be easily quantified and if this is attempted the measures could be contradictory in nature. He defines these elements 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 organize themselves and the manner in which they alter their environment (Jablonsky, 2001, 2010). Jablonsky thus inadvertently provided the foundation for the DIME acronym. Jablonsky also referred to the formula of Cline . (Cline, 1993) to develop a rough estimate of "perceived" national power that focuses primarily on a state's capacity to wage war.

From a modelling perspective, Jablonsky's (1997) paper provides two approaches towards national power, firstly, power as a constructed, dialogue between two states. Secondly, power as an empirical cataloguing of characteristics which, if found in the correct mix and quantity, would designate "national power". He also attempts to reconcile the two approaches (two different "ways of knowing" defined by Moses (Moses & Knutsen, 2012)) in his explanation of national power. The crux of Jablonsky's argument is that national power is not an absolute science but rather has to be calculated in accordance to numerous factors (intangible) and attributes (tangible), as illustrated in Figure 1. It is important to understand that the national power attributes can be seen as the power potential of the state, where national power is derived from how these attributes are synergized, contextualized and deployed against an adversary to ensure dominance.

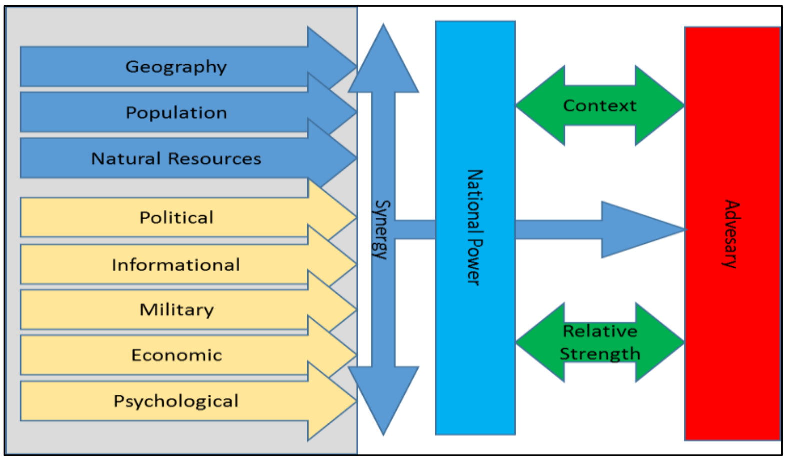

Figure 1: National Power

4. Cyberpower

Power based on information resources is not new; cyberpower is (Nye Jr, 2010). Cyberpower is also defined as the strategic employment of information and communications technologies to enable economic growth, empower society and enhance security (McConnell, 2012).

While cyberspace is the domain in which cyber operations take place, cyberpower is the sum of strategic effects generated by cyber operations in and from cyberspace. A definition often used is “cyberpower is the ability to use cyberspace to create advantages and influence events in other operational environments and across the instruments of power” (Kuehl, 2009). Spade defines cyberpower as “the ability of a nation-state to establish control and exert influence within and through cyberspace, in support of and in conjunction with the other domain-elements of national power. Attaining cyberpower rests on the state’s ability to develop the resources to operate in cyberspace” (Spade, 2012) .

Cyberspace and cyberpower are both dimensions of the informational instrument of power. The strategic purpose revolves around the ability to manipulate perceptions in your strategic environment to your advantage while at the same time degrading the ability of the adversary to comprehend that same environment. Cyberpower is thus the measure of the ability to manipulate that environment by access to the target’s cyber infrastructure via exploitation and attack (Sheldon, 2011). Cyberpower can also be seen as the capability to control IT systems and networks in and through the digital or cyberspace. Cyberpower is ingrained in the other elements and instruments of power. Cyberpower creates synergies between those elements and connects them in ways that most significantly and transformatively improve all of them (Zimet & Barry, 2009). The impact is that of linking people and organizations in the new wired world where traditional borders are being altered (Sheldon, 2011). Cyberpower is ubiquitous (Krekel & DeWeese, 2009; Sheldon, 2011), stealthy and with the fact that it is a complementary instrument, it forms the three main characteristics of this power. Although land, sea, air, and space power are able to generate strategic effect on each other, it is not as absolute and simultaneous as cyberpower due to the ubiquitousness characteristic of this power (Lonsdale, 2004). According to Sheldon, cyberpower has not proven to have a coercive capability, and thus can only be a complementary instrument. However the stealthyness makes it attractive to use (Sheldon, 2011).

Military cyberpower is defined by Zimet (2009) as the application of operational concepts, strategies, and functions that use the tools of cyberspace to accomplish military objectives and missions, and can be used in support of other domains, or on its own totally in cyber space (Zimet & Barry, 2009). Military power is one facet of national power which includes the economy as well as political and national will (Spade, 2012).

5. Cyberpower as part of national power

Cyberpower is one of the ways attributes can be unlocked to enable national power. It is an intangible source of power which acts as a catalyst and accelerator for national power (Zimet & Barry, 2009). Klimburg (Klimburg, 2011) discussed the Integrated National Capability Model for Cyberpower that takes into consideration a country's diverse non-state cyber elements that are used in direct support of government pollicies of a state. Cyber is mostly a non-state domain as the internet infrastructure (hardware), software programs, and web are mostly created and maintained by the non-state sector. This will have a influence on national power as Jablonsky points out how people (non state actos in Klimburg's case) look at life will influence how they organise and govern themselves, and all these elements weighed in relation to the problem of national security will influence the nature, size, and effectiveness of the armed forces (Jablonsky, 2001, 2010; Klimburg, 2011).

~~*5.1.1*~~5.1 Approaches

Formatted: Heading 2, Space Before: 0 pt, After: 0 pt, Line spacing: single

The key to determining cyberpower's contribution to national power is to determine its relationship to national power. Three broad approaches can be followed:

~~a.~~*5.1.1* *Cyberpower is an attribute or element of national power*

Formatted: Heading 3, Space After: 0 pt, Line spacing: single

- Cyberpower can be seen as an independent element of national power. The DIME framework can be extended to include a C for cyber as an element of national power. This can be done in two ways
  - Finding an element that strongly relates to cyber, such as "informational" or "psychological" and deal with cyber within that element, or
  - Giving cyber a status of an independent element or domain, such as the cyber domain (Murphy, 2010) (5th domain).

Formatted: Line spacing: single

Cyber is linked to all attributes of national power (Raymond, 2010). This is a very important concept; note that the National Defence University has a cyber certificate course focusedon understanding all the aspects of cyberspace and how to best integrate cyberspace with the all the other elements of national power to ensure the achievement of the nation's strategic objective (NDUi College, 2015).

~~b.~~*5.1.2* *Cyberpower is derived from synergizing all the attributes of national power, and is thus a way rather than a means of power.*

Formatted: Heading 3, Space After: 0 pt, Line spacing: single

This approach is to argue that cyberpower is a part of national power, and that cyber elements reside in each element of DIME, and as such then cyberpower is a layer of power that resides between national power and its elements (Betz & Stevens, 2011). This argument suggests that cyberpower is simply the exercise of power in a new context, rather than a new element of national power. This means cyberpower is more than simply a concrete capability. Although this radical formulation of cyberpower may sit uncomfortably with many cyber advocates, it does highlight an important idea that cyber is more than the sum of its parts. The relationship of cyberpower to the elements of power is similar to the relationship of the operational level of war to the tactical level of war. Cyberpower is somewhat elevated from, but not independent of the primary elements or attributes of national power (Betz & Stevens, 2011).

~~c.~~*5.1.3* *Cyberpower as a WAY of attaining national power*

Formatted: Heading 3, Space After: 0 pt, Line spacing: single

In this approach, cyber is accepted as an abstraction or a level of analysis, rather than a concrete tangible element. For this approach cyberpower is an abstraction (or set of attributes) derived from the interrelation of both the elements and the exercise of national power (Kramer & Starr, 2009). This results in cyber as a layer of understanding or experience that has become mankind's preferred interface with reality. The cyber terrain model of Riley is a multi-layered model that conceptualise the layers in the cyber terrain. He uses a 15 layer cyber terrain model that visualise the physical and logical parts of the cyber terrain (Riley, 2014). From this it can be concluded that cyber has become a layer of abstraction between man and reality.

~~5.1.2~~5.2 Perspectives of cyberpower

Formatted: Heading 2, Space Before: 0 pt, After: 0 pt, Line spacing: single

In order to incorporate cyberpower into Jablonsky's idea, three perspectives will be tested:

- Firstly, defining cyberpower as independent element of power within national power, effectively enlarging the DIME/MIDLIFE acronym, to include a C for cyber as an alternative view. (Military, intelligence, diplomatic, law enforcement, information, finance, and economic elements (MIDLIFE)). Cyberpower will be placed into the "DIME-P" (diplomacy, information, military economics- politics) framework as an element of national power. Declaring cyberpower as a dimension of an already defined element of national power allows for a "business as usual" attitude, and provides a solid point of departure for those familiar with the "DIME"/"MIDLIFE" acronym (Kuehl, 2009). This is aligned with the military doctrine of the "fifth domain". Kuehl, for instance, is insistent that the element most closely tied to cyberpower is information (Kuehl, 2009). Cyberspace and cyberpower are clearly dimensions of the informational instrument of power under the PIME (political, informational, military, economic) model. He however also indicates that that cyberpower links in many ways to, supports, and enables the creation and exercise of the other instruments of power. He also claims that cyberpower creates synergies across the other elements and instruments of power that connects them in ways that will improve all of them. This shows that cyber is not clearly just a dimension of the Informational element.
- Secondly, comparing cyberpower by using the indicators of the Booz Allen Cyberpower Index (2011) to the traditional "DIME" elements, shows that cyberpower is an abstraction of the DIME acronym, and thus cyber is a fractal of National Power and not an element. Furthermore, the Cyberpower Index defines cyberpower as "the ability to withstand cyberattacks and to deploy the digital infrastructure necessary for a productive and secure economy", and isolates the dimensions of the "cyber element" as "legal framework", "economic and social context", "technology infrastructure", and "industrial application". A brief review of the Cyberpower Index shows that many of the "building blocks" or elements of cyberpower are not informational or ICT at all, but are embedded in the other elements. Although it can be argued that the Index has an economic bias, what is clear is that "cyberpower" is as much derived from the elements of DIME as it "improves them all" (Booz Allan Hamilton, 2011).
- Lastly, to properly understand cyberpower, treating it as an element or subset of national power is insufficient. A more constructivist approach is required, as cyberpower, like national power, is derived not only from its elements but rather from the relationships between the elements, the adversary, the context and the desired outcome. Cyberpower is indeed a manifestation of national power rather than just an element. It should be evident from the discussion that cyber, although seen as a "fifth dimension" of war, is not necessarily sufficient independent of the elements of power (DIME) to be treated as a primary or base element of power. Cyberpower thus should be considered as abstractive in nature, a fusion of the primary elements.

6. National power formulation

Formulas to calculate national power were already generated in the early 20th century. Various measurement factors such as GDP, population size, population density and distance from centra, budget expenditures and other demographics (Höhn, 2014) were incorporated in these formulas. A distinction is made between the traditional approach, with emphasis on the exercise of judgement, and the scientific approach that uses logical or mathematical proof. Höhn (2014) discusses reasons regarding why the scientific approach is not necessarily the best way. The traditional approach is preferred above the scientific approach due to the fact that the latter approach limits itself to matters of marginal importance (Höhn, 2014). Although it is helpful in producing illustrative analogies, only the traditional approach can produce judgmental values. The scientific approach relies on the uncertain promise of a unified, objective international relations theory in the future, which may never be realized due to complexity, impossibility of controlled experimentation, constant change, and a holistic interchangeability of subject/object as well as cause/effect. These limitations are significant shortcomings when devising power formulas; they over simplify realities. A distorted picture can be created in the scientific method due to ignorance of qualitative differences in the units counted, and assuming that these differences may not cancel each other out. The demand for rigor and precision can be accommodated in the traditional approach by inclusion definitions of terms and procedures that conform to logic. The proponents of the scientific approach tend to ignore philosophy and history which makes a self-critical attitude towards their own assumptions impossible (Höhn, 2014). The authors of this paper thus decided to use the traditional approach to develop a formula for the calculation of the influence of cyber power on national power.

The total war paradigm that evolved in the cold war features three types of power, military, economic and psychological power. An accurate measure of national power has to include these factors (Höhn, 2014). Treverton & Jones (2005) argue that economic power is the foundation of military power with the GDP being the most important single indicator (Treverton & Jones, 2005). The GDP, on the other hand, provides only a limited picture on its own as it does not indicate the composition of the economy, where the economy is going (leading sectors) or if it is dominated by old or declining sectors. Other important variables to include are human capital and technology that can be measured by education levels and the per-capita expenditure on research and development. The resulting picture will, however, not provide a complete indication of power in 2020. Treverton (2005) argues further that the indicator is likely to have something to do with *quality and* the ability of states to convert these components into useable outputs (Treverton & Jones, 2005). There is, however, a lot of support in the scientific approaches for using GDP as the foundation for assertions for future power (Höhn, 2014).

Höhn also identifies Ray Cline's formula (Cline, 1993) for power as the best known power formula ever produced from an international view point (Höhn, 2014). This formula of Cline determines perceived power (Pp) using the population, economy, military and strategy into consideration:

$Pp = (C + E + M) \times (S + W)$ in which:
Pp = Perceived power
C = Critical mass: population and territory
E = Economic capability
M = Military capability
S = Strategic purpose
W = Will to pursue national strategy

In his study on the measurement of national power Höhn (2014) analysed several formulas used for the calculation of national power. Höhn then defined national power as:

$NP= (E+M) \times P$ in which:
NP=national power
E= economic factor
M=military factor
P=psychological factor

In this formula Höhn uses the psychological factor to combine the "Strategic Purpose and Will to pursue" from Cline's formula.

One of the lessons from the Cline formula for perceived power is that the more tangible elements (C, E, and M) can be quantified objectively, although it also involves varying degrees of subjective qualifications. The Cline formula of $Pp = (C + E + M) \times (S + W)$ also demonstrates that perceived national power is a product, not a sum of its components. It thus serves as a reminder of the importance of relational and contextual aspects. The formula of Höhn also shows the importance of the psychological factor used as a product in the formula as opposed to the summerisation of the other factors. Beaufres (1964) formulates strategy as a product of force, psychological factors time and other specific factors. This formula is defined as

Kx F x Ps x T where
K = specific factor
F = material force
Ps= psychological factor
T= time

7. Development of formula for National Cyberpower

Taking all these formulas into consideration, the approach in this paper is to create a formula similar to Cline's using the Jablonsky elements for national power and Höhn's simplified version of national power. The first part of the Cline formula refers to the capability of a country and the second part to will, strategy, or relative power. Using Jablonsky's discussion on national power pertaining to the formula of Cline, it can be represented as:

*Perceived power (PP) = Capability * (Will, Strategy) or*
*Perceived power (PP) = Capability * (Psychological)*

The product between the Capability and Will/ Strategy implies that without any of the two latter factors, there can be no national power. A reduction in any of these two factors will have a significant effect on the product.

To define national power, Jablonsky differentiated between natural and social determinants of power (Jablonsky, 1997). One must, however, also understand how these elements are interrelated. For instance, resources are a natural factor, but the degree to which they are used is determined socially. Population factors, in particular, cut across the dividing line between both categories. The number of people of working age in the population affects the degree of industrialisation of a nation, but the process of industrialisation, in turn, can greatly alter the composition of the population. Jablonsky also argues that each separate element can be analysed, but the effects of those elements on one another must be considered, indicating that these complexities are compounded because national power is both dynamic and relative (Jablonsky, 2010).

An approach to combine the Cline formula with the Jablonsky determinants, the capability elements in Cline can be replaced by Jablonsky's natural determinants as well as economic, military and informational powers. Jablonsky's elements of geography, resources, and population that are concerned with the number of people in a nation and the physical environment of these citizens can be compared to the critical mass in the Cline formula. The other capability elements will be added to have the total capability as part of the social determinants (political, informational, military, and economic). The rest of the social determinants will be part of the strategic purpose and will to pursue national strategy group in the formula from the Cline. The perceived power formula can be expressed as

Perceived Power = ((Natural Determinants) + Economic + Military + Informational) x (Political + Psychological)
Or
Perceived Power = ((Geography +Resources + Population) + Economic + Military+ Informational) x (Political + Psychological)

As discussed before, cyberpower is not necessarily simply a collection of attributes but can also be seen as a set of interrelationships between attributes. Cyberpower is a construct or abstraction of the attributes, a way of applying national power rather than a means of national power. In this way cyberpower, although reflective of the other attributes of power, has its own independent characteristics and nature. This approach suggests that cyberpower is an indicator of national power and that there is a strong correlation between the two. In the above formulas for perceived power, the informational was part of the capability category and mainly referred to communication and information as part of communication. Cyberpower cannot be accepted as either a sub-element or independent element of this national power formula. It is far more complex and integrated than a single element or attribute of national power. Elements of cyberpower can be found in all the other elements or attributes of national power. Cyberpower also includes the roles of non state actors that form a critical part of national critical infrastructure. The constructivist approach to determine cyberpower may be a better way to arrive at a formula using all the aspects addressed by Jablonski (context, relative strength and outcome).

Using this as the basis, perceived cyberpower as a contributor to national power can be expressed similarly to Perceived Power:

Perceived Cyberpower (PCP) = Capabilities x (Intention, Will) or
Perceived Cyberpower (PCP) = Capability * (Psychological)

Raymond (2010) indicates that although cyber is part of the information space, it is also part of all the other domains, Land, Air Sea and Space. A conclusion can be drawn that cyberpower is not an independent domain but rather layers of abstraction that touches all aspects of national power and human existence. Using social and other media cyber can also be used to influence people and change their will. Therefore

Cyber Power (CP) =∑ cyber elements in (Diplomacy, Information, Military, Economics) x ∑ cyber elements in (Strategy, Will)

From the above discussion, the formula for perceived cyberpower (PCP) using Cline's formula as basis can be adjusted to

*PCP=(C+E+M) *(S+W) + Interrelations (C, E, M)*

Where, pertaining to cyber:

- *C* = Critical Mass that includes the size and age of the population as well as the level of cyber-awareness of the population. This will also include the differences in cyber-awareness of geographical distributed population. (e.g. awareness in rural, semi-rural and urban areas). The citizens play a critical role in your national cybersecurity and therefore national security because citizens can be exploited to either divulge sensitive information or be part of a botnet or the enemy's attack. The number of the cyber experts in addition also have an effect.
- E = Economic includes the cyber infrastructure and critical information infrastructure development and access.. This also includes technical and other cyber support or cyber workforce available.
- M = Military includes the inclusion of cyber in military forces and the development of a cyber command or similar (cyber defence capability).
- S = Strategy includes the implementation of a national cyber strategy, prevention of cybercrime, and education systems for cyber.
- W = Will or influencing of people to use cyber responsibly (awareness) and the prevention of cybercrime.

Similarly, using Jablonsky's determinants of power, the formula for perceived cyberpower can then be formulated as

> *Perceived Cyberpower = ((Geography +Resources + Population) + Economic + Military+ Informational) x (Political + Psychological) + Interrelations (Geography, Resources, Population, Economic, Military, Informational, Political, Psychological)*

The ability to accept that cyber is an abstraction of the elements of power, and that there is more than one level of abstraction, allows the development of an approach which can build a conceptual bridge between the constructivist (intangible) part of national power and the empirical (concrete) part. This proposes that the way attributes are organized and synergized towards the objectives of power are as important as the elements and the outcome. Hughes and Hillebrand used a quantitative approach for the calculation of technology power where technology power (economic-technological capability) is the product of GDP and GDPCC (GDP per capita) (Hughes & Hillebrand, 2006). In addition, cyberpower may be a fractal of national power and can also be seen as a missing attribute that encompasses all other attributes. If cyber is in every level of the elements of national security (C,E,M,S and W) it can be argued that using the Jablonsky's dimensions for capability, the perceived national power formula can then be adjusted to

PP=(C+E+M)(S+W) *PCP*
PP = ((Geography +Resources + Population) + Economic + Military+ Informational) x (Political + Psychological) x PCP

8. Conclusion.

Jablonsky defined national security in terms of the respective elements of the power base of the state and the priorities that are seen as of vital and/or national interest. He categorises the elements of national power into natural determinants and social determinants. The effects of all these elements on one another must be considered, indicating that these complexities are compounded because national power is both dynamic and relative. Cline developed a formula for perceived power that takes into consideration the effects of the different elements of national power on one another is that that focus primarily on a state's capacity to wage war.

This paper acknowledges that cyberpower is a multifaceted phenomenon. Kuehl points out that there are three distinct layers of cyberspace and thus cyberpower, namely the physical, then informational and lastly the cognitive (Kuehl, 2009). This presentation neatly dovetails with the argument presented in this chapter. The argument is simply that for cyberpower to be seen in relation to national power (in accordance with the Cline (1993) formula) it needs to be reconciled to both the physical attributes (as represented by DIME) as well as the cognitive levels of abstraction that are included in the "Strategic purpose and National Will" or intangible part of the formula.

The argument is that the initial conceptualization of cyber power as either an independent attribute or an element of an existing attribute of national power is insufficient. This is largely because later conceptualization conceded that cyberspace had both its foundations and utility in all the attributes of national power.

It is also argued in this paper that cyberpower is both physical attributes and an abstraction or synergy of all these attributes and is thus cyber power is best understood more as a way of achieving national power, than simply a means or attribute of national power. Thus, for a formulation for perceived cyberpower (PCP) would be best expressed as a replication or fractal of national power, and not a unique independent attribute.

It was shown that cyberpower is not an isolated element of national power, but rather a set of characteristics that are embedded in all elements of national power. It can also be layered as a further abstraction of the relationships between these elements. Thus, cyber is inseparable to national power, and furthermore it may have a strong correlation to national power in general. For this perception of cyberpower, Cline's formula for perceived national power and Jablonsky's determinants of power are used to define a formula for perceived cyberpower for a nation.

9. References

Beaufres, A. (1964). A conception of strategy: Revue de défense nationale December 1963. *Survival, 6*(2), 61-66.

Betz, D., & Stevens, T. (2011). *Cyberspace and the State: Toward a Strategy for Cyber-power*: Routledge, for the International Institute for Strategic Studies.

Booz Allan Hamilton. (2011). *Cyber power index: findings and methodology*. Retrieved from http://www.boozallen.com/media/file/Cyber_Power_Index_Findings_and_Methodology.pdf

Cline, R. S. (1993). *The power of nations in the 1990s: a strategic assessment*: University Press of America.

Höhn, K. H. (2014). Geopolitics and the Measurement of National Power.

Hughes, B., & Hillebrand, E. (2006). *Exploring and shaping international futures*: Paradigm Publishing, Inc.

Jablonsky, D. (1997). National power. *Parameters, 27*, 34-54.

Jablonsky, D. (2001). National Power. In J. R. Cerami & J. F. Holcomb (Eds.), *US Army War College Guide to Strategy*: Strategic Studies Institute.

Jablonsky, D. (2010). National Power. In J. Bartholomess (Ed.), *The US Army War College Guide to National Security Issues* (4 ed., Vol. 1: Theory of War and Strategy, pp. 123-140): Strategic Studies Institute.

Klimburg, A. (2011). The whole of nation in cyberpower. *Georgetown Journal of International Affairs*, 171-179.

Kramer, F. D., & Starr, S. H. (2009). *Cyberpower and national security*: Potomac Books, Inc.

Krekel, B., & DeWeese, S. (2009). *Capability of the People's Republic of China (PRC) to Conduct Cyber Warfare and Computer Network Exploitation*: DIANE Publishing.

Kuehl, D. T. (2009). From Cyberspace to Cyberpower: Defining the Problem. In F. D. Kramer, S. H. Starr, & L. Wentz (Eds.), *Cyberpower and National Security (National Defense University)* (pp. 26-28). Washington: Potomac Books, Inc.

Lonsdale, D. J. (2004). *The nature of war in the information age: Clausewitzian Future* (Vol. 9): Psychology Press.

McConnell, J. M. (2012). The Road to Cyber-power: Seizing Opportunity While Managing Risk in the Digital Age. In B. A. Hamilton (Ed.), *Foreign Affairs* (pp. 162-183): Booz Allen Hamilton.

Moses, J., & Knutsen, T. (2012). *Ways of knowing: Competing methodologies in social and political research*: Palgrave Macmillan.

Murphy, M. (2010). Cyberwar War in the fifth domain. *The Economist, July,1 2010*.

NDUi College. (2015). Cyber Leadership (Cyber-L) program. Retrieved from http://icollege.ndu.edu/Academics/GraduatePrograms/CyberLeadershipProgram.aspx

Nye Jr, J. S. (2010). *Cyber power*. Retrieved from

Phahlamohlaka, J. (2008). Globalisation and national security issues for the state: Implications for national ICT policies *Social Dimensions Of Information And Communication Technology Policy* (pp. 95-107): Springer.

Raymond, J. W. (2010). *Functional Concept for Cyberspace Operations*. Air Force Space Command.

Riley, S. (2014). "Cyber Terrain": A Model for Increased Understanding of Cyber Activity. Retrieved from https://www.linkedin.com/pulse/20141007190806-36149934--cyber-terrain-a-model-for-increased-understanding-of-cyber-activity

Shehadey, B. D. (2013). Putting the "D" and "I" Back in DIME. Retrieved from http://inhomelandsecurity.com/putting-the-d-and-i-back-in-dime/

Sheldon, J. B. (2011). *Deciphering Cyberpower: Strategic Purpose in Peace and War*. Retrieved from http://www.au.af.mil/au/ssq/2011/summer/sheldon.pdf

Spade, J. M. (Ed.) (2012). *China's Cyber Power and America's National Security*. Carlisle Barracks, PA: U.S. ARMY WAR COLLEGE.

Steele, R. (2006). Information operations: Putting the "I" back into DIME. Carlisle, PA: US Army War College Strategic Studies Institute. Retrieved August 20, 2007.

Treverton, G. F., & Jones, S. G. (2005). *Measuring National Power.* Paper presented at the RAND Corporation conference proceedings series.

Zimet, E., & Barry, C. (2009). Military Service Cyber Overview. In L. K. Wentz, C. L. Barry, & S. H. Starr (Eds.), *Military Perspectives on Cyber power* (pp. 1-29). Washington, DC: Center for Technology and National Security Policy at the National Defense University.