A Model for Measuring Perceived Cyberpower

JC Jansen van Vuuren[1,2], Louise Leenen [1]
1 Defence Peace Safety and Security: CSIR, Pretoria, South Africa
2 University of Venda, Thohoyandou, South Africa
jjvvuuren@csir.co.za
lleenen@csir.co.za

Abstract: Cyber Defence is a core driver in the attainment of national security for any country. Perceived Cyberpower can be determined by the analysis of the elements of cyberspace as part of national security. In this paper the Perceived Cyberpower formula that formed part of the national security determinants and formula for Perceived National Power (PNP) (Jansen van Vuuren, Leenen, Plint, Zaaiman, & Phahlamohlaka, 2017) will be used determine the level of cyberpower of a country. Cyberpower is a multifaceted phenomenon: it consists of both physical attributes (as represented by diplomacy, information, military and economics) as well as the cognitive levels of abstraction that are included in the strategic purpose or intangible part of the Perceived Cyberpower formula. Cyberpower comprises both physical attributes and an abstraction or synergy of all these attributes and thus cyberpower is best understood as a way of achieving national power, rather than simply a means or attribute of national power. It is important to understand how these elements of cyber power interrelate because that also influences the measurement of cyberpower.

This paper presents a new methodology to create a model for the measurement of cyberpower. This new methodology is based on Saaty's Analytical Network Process (ANP), Zwicky's General Morphological Analysis (GMA) (Ritchey, 1998) and the Perceived Cyberpower formula (Jansen van Vuuren et al., 2017). Due to the absence of accurate values or comparable values, the judgements of knowledgeable experts can be used to rank the cyberpower of different countries. This paper shows how to measure cyberpower that represents the cyber environment of a country using the Perceived Cyberpower formula (Jansen van Vuuren et al., 2017).

Keywords: Cyber Power, National Security, Cyber Defence, National Power, Analytic Network Process

1. Introduction

Cyberpower, as defined by Langer, is a society's organized capability to leverage digital technology for surveillance, exploitation, subversion and coercion in international conflict (Langer, 2016). Cyber however is a multifaceted phenomenon with three distinct layers, physical, informational and cognitive (Jansen van Vuuren et al., 2017). In this paper, cyberpower includes the military as an attribute because in the context of national security context cyberspace is used for the attainment of national power. Although cyber is part of the information space, it is also part of all the other domains; Land, Air Sea and Space (Raymond, 2010) . 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.

The only index for cyberpower is the Cyber Power Index developed by Booz Allen Hamilton that focuses on policy, and organizational and technical aspects of cybersecurity (Booz Allan Hamilton, 2011). The goal of the Booz Allen Hamilton Cyber Power Index is to provide a benchmark of the ability of the G20 countries to withstand cyberattacks and to deploy the digital infrastructure needed for a productive and secure economy,. However, there is no reference to military power.

Several Indexes for Cybersecurity were developed over the years. The indices for countries include (International Telecommunications Union (ITU), 2017):

- The Cyber Maturity in the Asia –Pacific Region developed by Australian Strategy Policy Institute;
- The National Cybersecurity Index developed by the Estonian e-Governance Academy;
- The Global Cybersecurity Index developed by ITU;
- The Kaspersky Cybersecurity Index;
- The Asia –Pacific Cybersecurity Dashboard developed by BSA;

- The Cyber Readiness Index developed by Potomac Institute for Policy Studies (which includes military capabilities); and
- The Cyber Green Index that focuses mostly on technical threats.

As indicated earlier, the only cyberpower index currently available is that of Booz Allen and Hamilton (Booz Allan Hamilton, 2011). The Booz Allen Hamilton Cyber Power Index relies on experts from the economic intelligence unit as analysts to identify categories and indicators. The Index uses the four categories: Legal and Regulatory Framework, Economic and Social Context, Technology Infrastructure and Industry Application. Each category has several indicators and sub indicators. Data was obtained from quantitative indicators of national and international statistics and where data was not available, estimates were made. Indicators were rated on a scale of 0 to 4 (there were some exceptions). However, real values were used when available. The experts recorded their input on the relative value of each category and indicator. The weighting assigned to each category in these indicators can be changed to reflect different assumptions about their relative importance, but the default weightings were set to the experts defined weightings. Indicators for which a higher value means a more favourable cyber power environment, have been normalised. These normalised values are transformed from a 0-1 value to a 0-100 score. The overall Cyber Power Index is calculated from a simple average of the category and indicator scores. The problem with the Cyber Power Index is that the interrelations between the categories could not be modelled in such a hierarchical process. In addition, the military contribution is not taken into account.

An analytical method for dealing with a complex multi-criteria decision making problem is required to derive a model to measure cyberpower. The first choice was to use Saarty's Analytic Hierarchy Process (AHP) (T. L. Saaty, 1999). The AHP is a well-known multi-crieria decision making tool (Ravi, Shankar, & Tiwari, 2005) that structures a problem into a hierarchy with a goal, decision criteria and alternatives. However, AHP considers all elements in the hierarchy to be independent of all the others; it does not consider interrelationships and feedback between elements in a model. This shortcoming may result in misleading decision making (Piantanakulchai, 2005).

The Analytic Network Process (ANP), introduced by Saaty in 2004 as a generalization of the AHP, is a multicriteria measurement tool used to drive relative priority scales of absolute numbers from individual judgments (or from actual measurements normalized to a relative form) (T. L. Saaty, 2004). The ANP structures a problem as a network instead of a hierarchy, and it can capture the interdependencies between the criteria under consideration, hence allowing for a more systemic analysis. The ANP allows the inclusion of criteria, both tangible and intangible (difficult to quantify), which has some bearing on making the best decision. A pairwise comparison process is used to determine the relative influence of one of two elements over themselves as well as on a third element in the system, with respect to an underlying control criterion. The ANP synthesizes the outcome of dependence and feedback within and between clusters of elements with a supermatrix of which the entries are themselves matrices of column priorities. This tool overcomes the limitation of linear hierarchical structures and their mathematical consequences (T. L. Saaty, 2004). When factors have some level of interdependency among them, ANP modeling is a better fit because it includes modelling interrelationships. (Ravi et al., 2005).

The ANP relies mostly on judgements of experts when comparisons of elements are made and when the influences of elements on each other have to be determined. To support this phase of the ANP we use General Morphological analysis (GMA) (Ritchey, 1998). GMA is a well-known problem structuring technique aimed at solving complex problems. This form of non-quantified modelling relies on the judgmental processes of subject matter experts. GMA uses facilitated workshops (pre-workshop and workshop) with the group of subject matter (domain) experts that are able to address the specific problem complex. One of the principles of GMA is to identify the relationships and given uncertainties inherent in such multi-dimensional problem spaces and present this in a structured, reduced format, called a morphological field. The authors modified GMA slightly and used Modified GMA in this paper (Jansen van Vuuren et al., 2017).

2. Modelling Measurement of Cyber power

2.1 Analytic Network Process (ANP)

The ANP consists of two parts. The first part is to decide on the control hierarchy or network of criteria and sub-criteria that controls the interactions. The second part is to construct a network of influences among the elements and clusters. The pairwise judgments evaluate the relative influence of one of two elements over a third element in the system using the pairwise comparison process. The more dominant of the two elements influencing the third element is determined with respect to a specific criterion. This criterion used to make all comparisons, represents the impact and is also known as the control criteria. When an element has no influence on another element, its influence priority is assigned (not derived) as zero. The network normally varies from criterion to criterion. A priority vector is derived from the paired comparisons results in a priority vector to form a column in the supermatrix. For each of the control criteria, a different supermatrix of limiting influence is created, where components are compared according to their relative importance. Decisions are made after each one of these supermatrices are weighted by the priority of its control criterion and the results are synthesized through the addition for all the control criteria. This weighted supermatrix or stochastic matrix thus includes comparison of clusters according to their impact on each other with respect to the general control criteria (T. L. Saaty, 2004).

Modelling a problem with the ANP can be described in the following steps.
Step 1: Problem formulation (Piantanakulchai, 2005):

- Modelling of the problem as a network
    - Describe the problem statement and identify the elements. The elements are the entities that interact with each other in the system and include the criteria, sub-criteria, and alternatives. The decision makers and stakeholders can also be elements.
    - Group the elements into clusters. A cluster is a group of elements with a common characteristic. Note that in a complex system with a large number of elements, it may not be viable to compare all the elements with each other. Elements that share characteristics can be grouped in a cluster.
- Construct the network.
- Analyze the influences in the network. Determine the clusters that influence the elements in a selected cluster. The dependencies are either relations or feedback between elements.

Step 2: Structure the Influence matrix (da Silveira Guimarães & Salomon, 2015):

- Construct an influence matrix (supermatrix without weights), which lists all the elements arranged in their clusters by laying out the clusters in the order they are numbered and all the elements in each cluster both vertically on the left and horizontally at the top.

Step 3: Do pairwise comparisons (R. W. Saaty, 2016). The comparisons are done on two levels:

- Pairwise comparison is done on elements in the clusters based on their influence on other elements in the same cluster (inner dependence) or elements they are connected to in another cluster (outer dependence). All comparisons are done based on a criterion, and when the comparison concerns the extent of influence other elements have on a given element, a control criterion or sub-criterion of the control hierarchy drives the comparison.
- Comparisons have to be made on clusters based on the influence they have on other clusters to which they are connected. If there is no influence a weight of zero is assign, otherwise derived weights are included in the supermatrix to get the weighted column supermatrix. The supermatrix is equal to the influence matrix multiplied by the priorities of the clusters. Columns are normalized.
- Do consistency checking.

Step 4 : Compute the limit supermatrix and determine the result (the global priority of each element of the network) (R. W. Saaty, 2016).

- Perform sensitivity analysis on the final outcome and interpret the results of sensitivity by noting how stable this outcome is. Compare it with the other outcomes by taking ratios and observing how large or small these ratios are.

In this paper, the ANP process is used because it is capable to model interrelations. In cases where exact data is not available, the judgements via pairwise comparisons can be used to model subjective indications. In the case of these pairwise comparisons, a geometric mean will be used to calculate an average index from the experts' judgements for implementation in the model.

2.2 General Morphological Analysis

GMA is a non-quantified modelling method for structuring and analysing ill-structured problems that contain uncertainties and require a judgemental approach. This method builds an inference model that strives to represent the total problem space and a maximum number of possible solutions. The GMA methodology comprises a number of iterative steps, in which a subject specialist or focus group iterates through a number of analysis and synthesis cycles. A morphological analysis is carried out in two phases. The Analysis phase defines the problem complex in terms of variables and variable conditions. During the analysis phase, the most important dimensions of the problem are identified and defined. Each dimension (or parameter) is given a number or a range of values or conditions. A multi-dimensional configuration space is constructed (called a morphological field) by setting these parameters against each other, with each as the heading of a column and its values in the rows. One state (or solution) of the problem is found by selecting one value from each column. A morphological field represents the total solution space and thus can have many possible solutions. The Synthesis phase links variables and synthesises an outcome space. In a synthesis cycle, the participants reduce the number of possible solutions by doing a Cross-Consistency Assessment (CCA): every pair of values in the morphological field is checked for consistency. The set of possible solutions is reduced to contain only internally consistent configurations. Note that the success of GMA depends on the availability of a group of subject specialists. The output of GMA is no better than the quality of its input. The following references can be consulted for more information and detailed descriptions of GMA ((Ritchey, 1998); (Ritchey, 2002)).

The modified GMA (MGMA) follows similar steps to the GMA, but in the MGMA process, facilitators are allowed to contribute knowledge during the preparation phase by pre-selecting certain variables (Jansen van Vuuren et al., 2017).

2.3 Perceived Cyberpower

The Perceived Cyberpower formula, used in this paper to define cyberpower, is based on the Jablonsky formula for perceived national power and the Cline formula for national power as presented by Jansen van Vuuren et al. (Jansen van Vuuren et al., 2017). The formula used for the measurement of Perceived Cyberpower for this paper is:

Perceived Cyberpower=(C+E+M+I) *(S+W) + Interrelations (C, E, M,I)

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, technology 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).
- I = Informational. Includes communication and information from systems and technology or the lack of access due to unavailability of systems.
- S = Strategy includes the implementation of a national cyber strategy, prevention of cybercrime, and education systems for cyber.(includes legal and regulatory frameworks)
- W = Will or influencing of people to use cyber responsibly (awareness) and the prevention of cybercrime.

To determine cyberpower, index indicators need to be developed for the above categories.

3. Model for the measurement and ranking of Perceived Cyberpower

As previously indicated, the ANP is also a tool to gain deeper insight into a complex decision problem (Goepel, 2011) and MGMA is a tool to model complex problems. To model the measurement and ranking of cyberpower, a combination of the ANP and MGMA methods are used.

Klaus Goepel (Goepel, 2011) indicates that the development of the ANP model is the most difficult part of the process. To set up the model you need to:

- Give careful consideration and a clear description of the decision problem.
- Do thorough brainstorming to find important criteria and relevant factors.
- Clarity criteria and factors and define their exact meanings. (Keep the number of factors between three and five in a cluster).
- Do a systematic investigation of interconnections between nodes.
- Simplify the model. If there is large number of factors, use comparisons to eliminate some of the factors).
- Perform a critical assessment of results.

The MGMA model is an excellent model to gain insight in complex problems. With the use of a MGMA model, the difficulty of steps 1 and 2 of the ANP (as described by Goepel above) can be simplified. We therefore suggest a combined model of ANP and MGMA for modelling the measurement of Perceived Cyberpower. The combined methodology Modified General Morphological Analytical Network Process is set out in Figure 1.

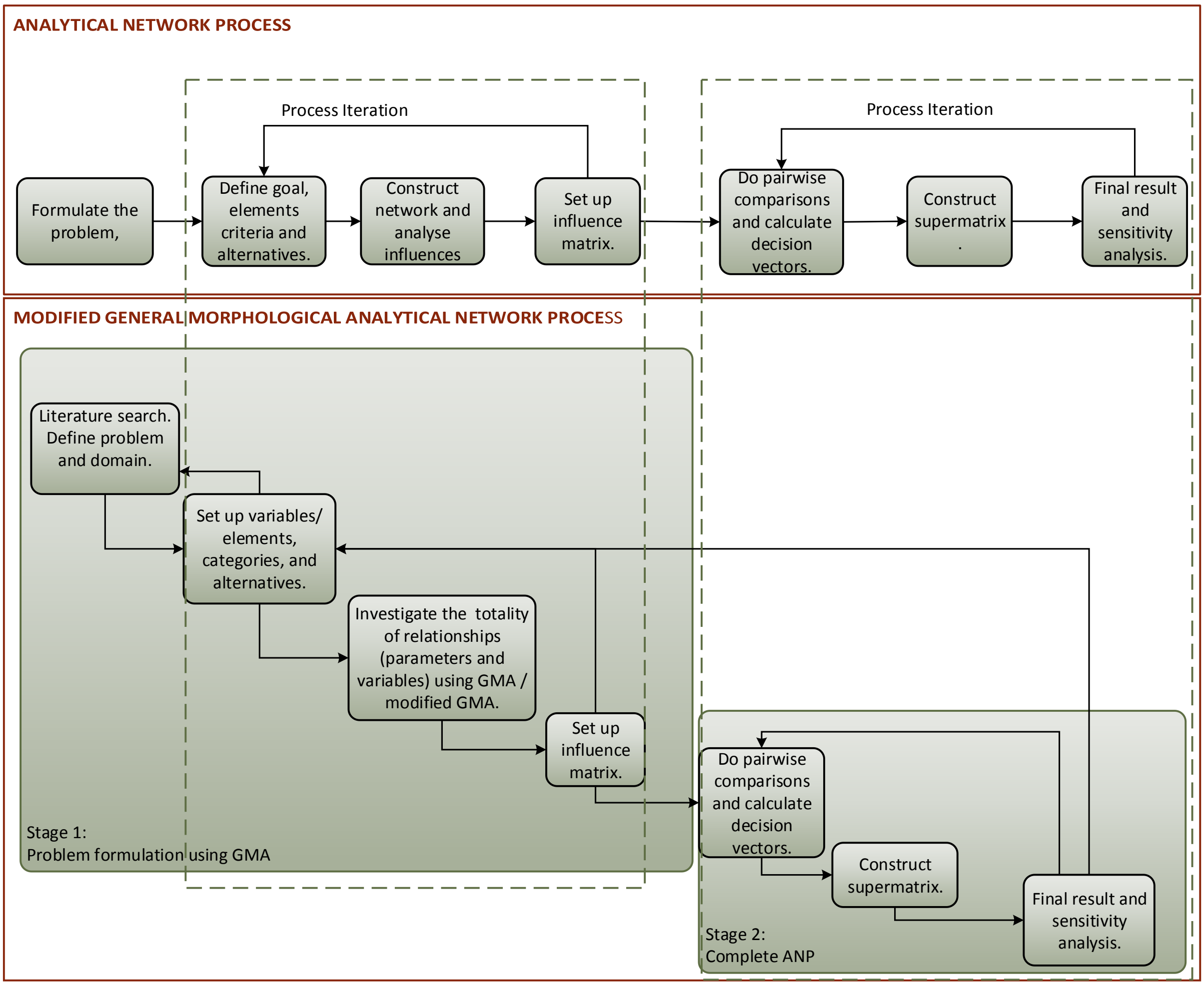
ANALYTICAL NETWORK PROCESS
Process Iteration
Process Iteration
Formulate the problem,
Define goal, elements criteria and alternatives.
Construct network and analyse influences
Set up influence matrix.
Do pairwise comparisons and calculate decision vectors.
Construct supermatrix .
Final result and sensitivity analysis.
MODIFIED GENERAL MORPHOLOGICAL ANALYTICAL NETWORK PROCESS
Literature search. Define problem and domain.
Set up variables/ elements, categories, and alternatives.
Investigate the totality of relationships (parameters and variables) using GMA / modified GMA.
Set up influence matrix.
Stage 1: Problem formulation using GMA
Do pairwise comparisons and calculate decision vectors.
Construct supermatrix.
Final result and sensitivity analysis.
Stage 2: Complete ANP

Figure 1: Modified General Morphological Analytic Network Process

3.1 Implementation of the model.

3.2 Steps 1-2 ANP model

The first step in the modelling of the Perceived Cyberpower includes the identification of categories and the set-up of relationships. The Modified General Morphological Analysis technique can be used to identify these categories. It should be noted the all feedback dependencies require experts in multi-disciplinary fields to ensure they are able to judge the relative importance of upper level criteria with respect to a single lower criterion or indicators (Piantanakulchai, 2005). Therefore an expert will base his preferences on his knowledge field and his input on the other fields will be adjusted with pressure from other experts (inner dependence). If, for example, all the experts are military experts the input will be biased on military capability only. This can influence the relative weights significantly.

The Perceived Cyberpower formula consist of two clusters, the Capability and Influencing/diplomacy, each with different elements as shown in Figure 2.

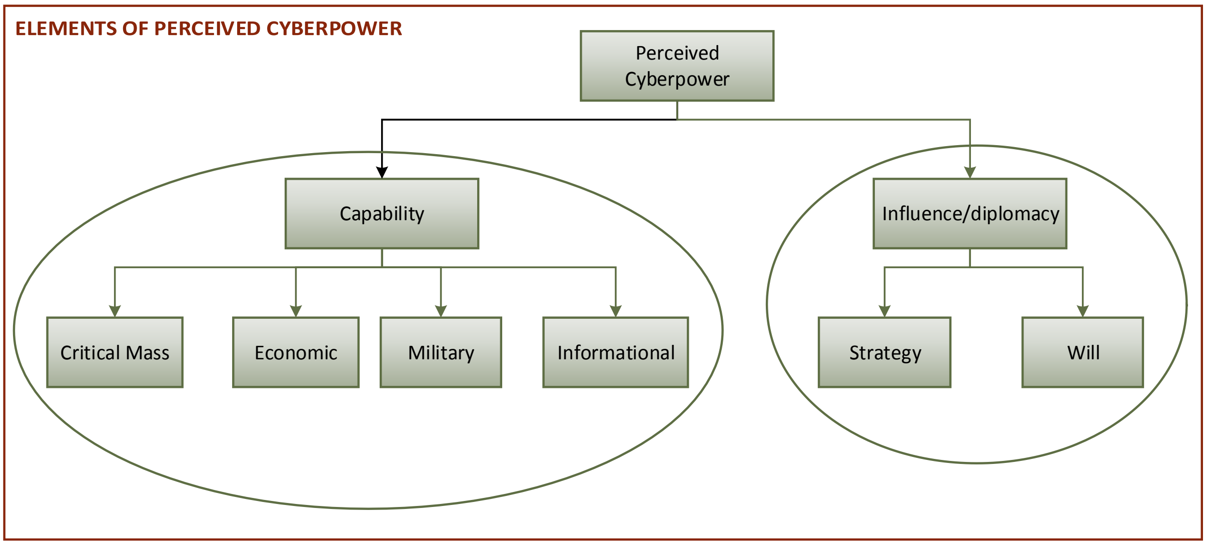

Figure 2: Perceived Cyberpower Elements

The elements of the Perceived Cyberpower formula in Figure 2 (and in Table 1) are used as input to the MGMA exercise. The authors have made progress with these steps but the MGMA still has to be completed. Intermediate results are shown. During the exercise the clusters, criteria and subcriteria are identified as well as the alternatives to be used for the model. For each of the clusters a separate MGMA table and cross consistency matrix must be completed. The information gained from the MGMA for cluster 1 (capability) is reflected in

Table 2. For the benefit of writing this paper, the categories identified by Booz Allen Hamilton (2011) , as well as other literature review resources e.g. Inkster (2017), Klimburg (2011) and Aschman (2015) were used to determine the criteria and sub-criteria of the elements displayed in Table 2. The relationships between Elements and Subcriteria will be represented in the Cross-Consistency Matrix which is not shown in this paper. The MGMA cross-consistency matrix is then used to determine both the interrelations in the network as well the knowledge needed to complete the influence matrix.

Table 1: Elements of Perceived Cyberpower Formula Used in MGMA

Capability	Critical Mass (C)
	Economic (E)
	Military (M)

	Informational (I)

Table 2: Elements, Criteria, Subcriteria and Alternatives as Identified by the MGMA Model

Elements	Criteria	Subcriteria
Critical Mass (C)	Educational levels	• Tertiary student enrolment as a percentage of total enrolment • Expected years of education • English Literacy
	Technical skills	• Labour productivity growth • Researchers in research and development per million people • Cybersecurity, Computer Science and Engineering graduates
Economic (E)	Trade	• Information and communications technology exports as a percentage of total exports • Information and communications imports as a technology percentage of total imports • Openness to trade
	Innovative environment	• Research and development as a percentage of gross domestic products • Domestic patent filings • Private equity and venture capital as a percentage of gross domestic product • Smart Grids
	E-Commerce and Governance	• Intelligent transportation • E-Health • Placement of orders via internet(business and individual) • Financial (internet banking etc)
Military (M)	Cyber capability developments	• Military research facilities • Military cyberwarfare education institutions • Cyber Range for training • Access to non-state actors
	Cyber and Intelligence Operations Capability	• Cyber Defence Strategy • Military Cyber Units (Cyber Command / Cyber Army) • Cyber Weapons
Informational (I)	Access to information and Communication technology	• Internet penetration • Mobile cellular penetration • Wifi hotspot per million people • Social media penetration
	Quality of information and communication technology	• Internet bandwith
	Affortability of Information and Communication Technology	• Mobile phone tariffs • Broadband Internet tariffs • Information technology spending as a percentage of GDP
	Secure servers	• Software and hardware protective measure • Regular vulnerability testing • Resilience programs

The ANP network model (step 1) in the ANP process is created using the results of the MGMA that includes the criteria and subcriteria, alternatives and inter relations between the elements. As indicated before, inter dependencies and outer dependencies between the criteria and subcriteria can be modelled by using the results of the cross-consistency matrix of the MGMA. The resulting ANP network model is given in Figure 3. The influence matrix can also directly be populated by using the results of the cross-consistency matrix of the MGMA. The Influence matrixes will be set up for the cluster *Capability* and the cluster *Influencing/Diplomacy*.

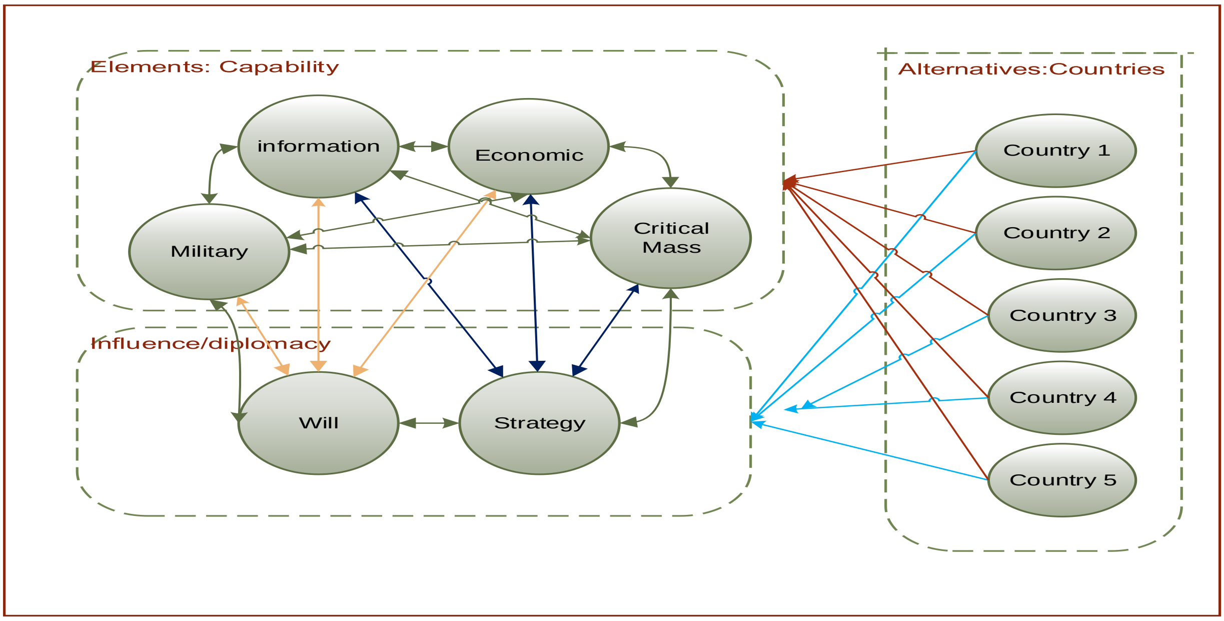

Figure 3: The ANP Network for Perceived Cyberpower

3.3 Steps 3-4 of the ANP model

The remainder of the ANP process should now be completed, i.e. doing the pairwise comparisons and determining the weight vectors. It is important to do the consistency checking as well. If all the experts were part of the MGMA exercise, the results from the pairwise comparisons can be directly implemented. When different groups of experts are used, a geometric mean must be calculated to determine pairwise comparisons. The supermatrix is then be implemented using the eigenvectors obtained from cluster level comparison with respect to the control criterion applied as the cluster weights. The resulting matrix is normalized so that each of the columns of the matrix will sum up to unity. A sensitivity analysis can then be performed to ensure acceptable results.

4. Conclusion

Although cyberpower is an accepted indicator of national security, the means to measure the cyberpower of a country is an obstacle that is often raised by researchers and other experts in the domain. In this paper a new methodology, Modified General Morphological Analytical Network Process, is introduced to measure and rank the cyberpower levels of different countries. This methodology is based on the Modified General Modified Analysis (MGMA), the Analytical Network Process (ANP) and the Perceived CyberPower formula. This methodology is applied using the elements described in the Perceived Cyberpower formula and the judgements of knowledgeable experts.

The authors are continuing to refine the study, and due to the absence of accurate data, information from other studies were also included in the paper. The authors also present intermediate results of a MGMA process to identify the network (goal, criteria subcriteria and alternatives) required for the ANP phase of the process. The authors' intention is to test the methodology early in the next quarter. Invitations for the MGMA phase will be done with experts from the military, public and private sectors to include the whole spectrum of cyber. These results will be used in the modelling of the ANP. The final results of the study and the usefulness of the method will be discussed in the next paper.

5. References

Aschmann, M., Jansen van Vuuren, J. C., & Leenen, L. (2015). Towards the establishment of an African Cyber-Army. *The Journal of Information Warfare, 14*(3).

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

da Silveira Guimarães, J. L., & Salomon, V. A. P. (2015). ANP applied to the evaluation of performance indicators of reverse logistics in footwear industry. *Procedia Computer Science, 55*, 139-148.

Goepel, K. D. (2011). AHP-ANP practical Application with Pros and Cons. Retrieved from https://bpmsg.com/ahp-anp-practical-application-with-pros-and-cons/

Inkster, N. (2017). Measuring Military Cyber Power. *Survival, 59*(4), 27-34. doi:10.1080/00396338.2017.1349770

International Telecommunications Union (ITU). (2017). INDEX OF CYBERSECURITY INDICES 2017. Retrieved from https://www.itu.int/en/ITU-D/Cybersecurity/Documents/2017_Index_of_Indices.pdf

Jansen van Vuuren, J. C. , Leenen, L., Plint, G., Zaaiman, J. J., & Phahlamohlaka, J. (2017). Formulating the Building Blocks for National Cyberpower. *International Journal of Cyber Warfare and Terrorism (IJCWT), 7*(3).

Klimburg, A. (2011). Mobilising cyber power. *Survival, 53*(1), 41-60.

Langer, R. (2016). Cyber Power: An emerging factor in national and international security. *Journal of International Relations and sustainable development. HORIZONS: Global Security Challenges, Autumn 2016*(8).

Piantanakulchai, M. (2005). *Analytic network process model for highway corridor planning.* Paper presented at the Proceedings of the 8th International Symposium on the Analytic Hierarchy Process.

Ravi, V., Shankar, R., & Tiwari, M. (2005). Analyzing alternatives in reverse logistics for end-of-life computers: ANP and balanced scorecard approach. *Computers & industrial engineering, 48*(2), 327-356.

Raymond, J. W. (2010). Functional concept for cyberspace operations. Retrieved from http://info.publicintelligence.net/USAF-CyberspaceOpsConcept.pdf

Ritchey, T. (1998). *General Morphological Analysis, a general method for non-quantified modeling.* Paper presented at the 16th EURO Conference on Operational Analysis,, Brussels.

Ritchey, T. (2002). Modelling complex socio-technical systems using morphological analysis. *Adapted from an address to the Swedish Parliamentary IT Commission, Stockholm*.

Saaty, R. W. (2016). Decision Making in Complex Environments: Super Decisions Software for Decision Making with Dependence and Feedback. Pittsburgh, PA: Super Decisionss.

Saaty, T. L. (1999). *Fundamentals of the analytic network process.* Paper presented at the Proceedings of the 5th international symposium on the analytic hierarchy process.

Saaty, T. L. (2004). Fundamentals of the analytic network process — Dependence and feedback in decision-making with a single network. *Journal of Systems Science and Systems Engineering, 13*(2), pp 129–157.