2016 8th International Conference on Cyber Conflict
Cyber Power
N.Pissanidis, H.Rõigas, M.Veenendaal (Eds.)
2016 © NATO CCD COE Publications, Tallinn

Assessing Cyber Power

Jelle van Haaster
Faculty of Military Sciences
Netherlands Defence Academy, Breda
University of Amsterdam
j.vanhaaster@uva.nl

Abstract: This paper aims to contribute to the debate regarding quantitative and qualitative appreciation of cyber power. It will do so by: (1) deriving a thorough foundation for the cyber power discussion from the 20th century power debate; (2) presenting a comprehensive framework for analysing (cyber) power; and (3) positioning cyber capacities within this framework. Revamping the 20th century power discussion is necessary as the current cyber power debate focuses much on the 'means' component of power (e.g. DDoS capacity, network infrastructure spending, malware acquisition budgets, etc.). This view of power is very similar to the pre-World War II approach to assessing power. The power theorists, however, have shied away from this approach as it proved to be too narrow. Primarily because it failed to capture why a more resourceful actor sometimes fails to ascertain its objectives or preferred outcomes vis-à-vis a smaller actor (e.g. the United States' experience in Vietnam). In order to fill this lacuna, this paper offers a more comprehensive approach to power, including all dimensions of (cyber) power, being: scope, domain, weight, costs and means.

Keywords: *power, cyber power, quantification, cyber arms race, international relations*

1. INTRODUCTION

States relish comparing their own power with that of other states. When it stacks up, there is no need to worry, but whenever it appears to fall short it is deemed an omission requiring attention. Seemingly empiric quantification of power drives this type of governmental decision-making. By quantifying power, the feasibility and probable efficacy of a particular action can be determined. Statements about feasibility and efficacy are based on the notion that more powerful states, in whatever respect, are more likely to be able to advance their goals than weaker states.

Ranking of states on whatever basis frequently occurs, either by states or in the media. These forms of categorisation, qualitative appreciation, and quantification of power and power

resources at a state's disposal received considerable academic attention throughout the twentieth century. Although power and its quantification remain unsettled issues within the study of international relations, the contours of the discussion have settled.

Faced with new possibilities, challenges, and risks of interconnection on unprecedented scale, new questions arise with regard to the use and quantification of power, particularly questions about conveying power in or through cyberspace. Contemporary scholarly research expresses that cyberspace serves as a potent conduit through which power can be conveyed. It has not, however, addressed issues with regard to feasibility and efficacy of a particular course of action, or the preceding assessment of the distribution of cyber power. The contemporary cyber power debate seemingly also omits the power debate from the 20th century. Instead of using the conclusions of this debate, many use a pre-World War II approach to power, namely, that power is epitomised in control over resources. In order to fill this lacuna this paper will revamp the 20th century power discussion and adjoin it with contemporary insights regarding cyber power and capacities.

This paper will first briefly describe the essential elements of the twentieth century power discussion regarding the quantitative and qualitative appreciation of power. Section 2 will conclude with a conceptual framework for analysing power. After that, the paper will highlight the contemporary cyber power discussion in Section 3. In doing so, this paper will discuss various viewpoints on cyber power's quantitative and qualitative assessment. In Section 4, the framework for analysing power developed in Section 2 will be adjoined with contemporary notions regarding cyber capacities. In doing so, this paper will provide: (a) a basis for further discussion about cyber power not omitting more than a hundred years of power debate; (b) footholds for analysing cyber power; and (c) a viewpoint on the categorisation of cyber capacities within the power debate.

2. POWER

Within international relations, the concept of power is one of the most contested issues.[1] Even though 'weighty books have analysed and elaborated the concept',[2] much is unsettled apart from a notion that the issue requires attention.[3] It especially requires attention in the context of this paper, which seeks to present how cyber power can be assessed.

Comparing one's power to another has been a core activity for rulers from antiquity until now. Describing power as a concept and determining how to measure it is a more 'recent' development beginning in the late 18th century. Although seen from an entirely different *zeitgeist*, the mid- and late-20th century power debate has yielded valuable insights. This section will first briefly discuss different viewpoints on power derived from that discussion and then examine perspectives on assessing power.

This section will only cover Barnett and Duvall's categorisation of power's operation as it captures the most important viewpoints of the 20th century power discussion. Their insights

1 David A. Baldwin, 'Power and International Relations,' in *Handbook of International Relations*, eds. Walter Carlsnaes, Thomas Risse and Beth A. Simmons (London: Sage, 2002), 177-191. p.177.
2 Robert Gilpin, *War and Change in World Politics* (Cambridge: Cambridge University Press, 1983). p.13.
3 Ronen Palan, *Global Political Economy: Contemporary Theories* (London: Routledge, 2000). pp.53-54.

are based upon many fundamental post-World War II viewpoints on power.[4] This paper will not touch upon the pre-World War II viewpoints on power other than to observe that the notion at the heart of this 'elements of national power' approach was that a specific amount of power in the form of resources can be possessed, that the actor with most resources is most likely to forward their interests, and hence is more powerful.[5]

2.1 The operation of power

Where and how does power manifest itself? Debate regarding this question has been going on from the 1960s in the form of the faces of power (or power dimensions) debate, and has quite recently resulted in the more modern 'taxonomy of power concepts framework' described by Barnett and Duvall.[6]

Barnett and Duvall distinguish four types of power:

- Compulsory, epitomising 'power as relations of interaction of direct control by one actor over another';
- Institutional, considering 'the control actors exercise indirectly over others through diffuse relations of interaction';
- Structural, expressing 'the constitution of subjects' capacities in direct structural relation to one another'; and
- Productive, entailing the 'socially diffuse production of subjectivity in systems of meaning and signification'.[7]

This subsection will briefly describe these four power concepts.

Compulsory power follows the Dahlian definition of power: 'the ability of A to get B to do what B otherwise would not have done'.[8] It is very similar to the first face of power, and hinges on the intentionality, conflict, and successfulness of A.[9] Both state and non-state actors can exert compulsory power, 'multinational corporations can use their control over capital to shape the foreign [and global] economies' and 'non-state networks and groups sometimes […] terrorise entire populations'.[10] Compulsory power does not require material resources: 'it also entails symbolic and normative resources'.[11]

4 See for instance: Robert A. Dahl, 'The Concept of Power,' *Behavioral Science* 2, no. 3 (1957), 201-215.; Robert A. Dahl, 'A Critique of the Ruling Elite Model,' *The American Political Science Review* 52, no. 2 (1958), 463-469.; Klaus Knorr, *The Power of Nations: The Political Economy of International Relations* (New York: Basic Books, 1975).; Harold Hance Sprout and Margaret Tuttle Sprout, *Foundations of International Politics* (New Jersey: Van Nostrand, 1962).

5 See for instance: Hans J. Morgenthau, *Politics among Nations: The Struggle for Power and Peace* (New York: Alfred A. Knopf, 1948).; Hans J. Morgenthau, *Dilemmas of Politics* (Chicago: University of Chicago Press, 1958).; Quincy Wright, *A Study of War: Volume II* (Chicago: The University of Chicago Press, 1942).; J. D. Singer and Melvin Small, 'The Composition and Status Ordering of the International System: 1815-1940,' *World Politics* 18, no. 2 (1966), 236-282.; Frank H. Simonds and Brooks Emeny, *The Great Powers in World Politics: International Relations and Economic Nationalism* (New York: American Book Company, 1937).; A. F. Pollard, 'The Balance of Power,' *Journal of the British Institute of International Affairs* 2, no. 2 (1923), 51-64.

6 Michael Barnett and Raymond Duvall, 'Power in International Politics,' *International Organisation* 59, no. 1 (2005), 39-75.

7 Ibid. p.43.

8 Dahl, *The Concept of Power*. pp.202-203.pp.202-203.

9 Barnett and Duvall, *Power in International Politics*. p.49.

10 Ibid. p.50.

11 Ibid. p.50.

Institutional power involves an:

> 'actors' control of others in indirect ways […] the conceptual focus here is on the formal and informal institutions that mediate between A and B, as A, working through the rules and procedures that define those institutions, guides, steers, and constraints the action (or non-actions) and conditions of existence of others'.[12]

In such a scenario, A does not exercise power directly over B, 'A cannot necessarily be said to 'possess' the institutions that constraints and shapes B', but A could be the dominant actor 'that maintains total control over an institution'.[13]

Structural power 'concerns the structures – or, more precisely, the co-constitutive internal relations of structural positions – that define what kinds of social beings actors are'.[14] It 'concerns the determination of social capacities and interests' of actors, based upon the notion 'that the structural position of A exists only by virtue of its relation to the structural position of B'.[15] It 'is the production and reproduction of internally related positions of super- and subordination, or domination, that actors occupy'.[16] Structural power is best characterised by Steven Lukes' statement that it is 'the supreme and most insidious exercise of power' to prevent or permit actors from arising within societies or structures.[17]

Productive power is based on more or less 'generalised and diffuse social processes', unlike structural power that is based on direct structural relations.[18] Productive power 'is the constitution of all social subjects with various social powers through systems of knowledge and discursive practices of broad and general scope'.[19] In other words, productive power looks beyond structures, it is concerned with 'the social processes and the systems of knowledge through which meaning is produced, fixed, lived, experienced and transformed',[20] but also how discursive processes and practices produce social identities and capacities'.[21] Examples of productive power is 'the discursive production of subjects by using categories of classification such as 'civilised, rogue, European, unstable, Western, and democratic states'.[22]

2.2 Assessing power

The power of states was deemed to be easily measurable in the eighteenth century.[23] Factors taken into account were 'territory, wealth, armies and navies'.[24] The eighteenth century concept of quantifiable power based on resources has played a prominent role throughout history. Although some additions have been made, many decision-makers and political theorists still

12 Ibid. p.51.
13 Ibid. p.51.
14 Ibid. pp.52-53.
15 Ibid. p.53.
16 Ibid. p.55.
17 Peter Digeser, 'The Fourth Face of Power,' *The Journal of Politics* 54, no. 4 (1992), 977-1007. p.979.; Barnett and Duvall, *Power in International Politics*, 39-75. p.53.
18 Ibid. p.5.
19 Ibid. p.55.
20 Ibid. p.55.
21 Ibid. p.56.
22 Ibid. p.56.
23 *Baldwin, Power and International Relations*. pp.177-178.
24 Ibid.

believe that a state's power position can be derived from its sources of power, and that power can be possessed, stored, and collected.[25]

The 'relational power approach' conceives power and its measurability differently from the 'elements of national power approach'. Proponents of this approach argue that power should be defined relationally: it 'does not reside in a resource but stems from the particular relation in which abilities are actualised'.[26] Power is only meaningful 'if its control is seen to be valued by other actors in the interaction'.[27] Within this approach power is deemed multidimensional[28] and dependent of 'specific policy-contingency frameworks'.[29] This subsection will briefly describe these aspects.

Power is multidimensional. It consists – at least – of the dimensions of scope and domain.[30] Less accepted domains are dimensions such as weight, costs, and means.[31] The scope of power is understood to comprise objectives and the affected issue areas.[32] Domain 'refers to the […] actors subject to [the] influence [attempt]'[33] or simply 'the target[s]'.[34] Weight relates to the potential effectiveness of power; that is, the likelihood that 'B's behaviour is or could be affected by A'.[35] Costs indicate both the cost to actor A and the costs to B; for instance 'is it costly or cheap for A to influence B? Is it costly or cheap for B to comply with A's demands?'[36] Means refer to the various instruments 'of exercising influence', there are 'many ways to categorise such means', and these various instruments will be discussed in section four.[37]

Any statement about power would be meaningless without 'the specification of the situation' or the context.[38] Specifying the context is 'the single most important step in capability analysis' and basically entails 'establishing who is trying to get whom to do what' and in what situation.[39] Some power resources may be useless in one situation, whilst being extremely influential in others, 'the only way to determine whether something is a power resource or not is to place it

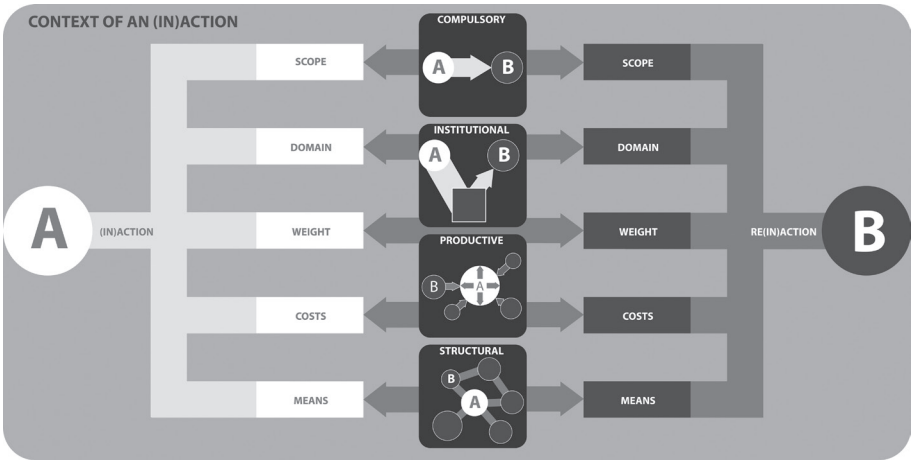
25 See for instance: Morgenthau, *Politics among Nations: The Struggle for Power and Peace.*
26 Stefano Guzzini, 'On the Measure of Power and the Power of Measure in International Relations,' *DIIS Working Paper*, no. 28 (2009). p.7.
27 Stefano Guzzini, 'Structural Power: The Limits of Neorealist Power Analysis,' *International Organisation* 47, no. 3 (1993), 443-478. pp.452-453.
28 Baldwin, *Power and International Relations*. p.178.
29 Guzzini, *Structural Power*. p.453.
30 Harold D. Laswell and Abraham Kaplan, *Power and Society: A Framework for Political Inquiry* (New Haven: Yale University Press, 1950). p.74.; Baldwin, *Power and International Relations*. p.179.; Joseph S. Nye, *The Future of Power*, 1st ed. (New York: Public Affairs, 2011). p.6.; Dahl, *The Concept of Power*. p.203.
31 Baldwin, *Power and International Relations*. p.178.; See also: Laswell and Kaplan, *Power and Society: A Framework for Political Inquiry*. p.74. They describe the dimensions domain, scope, weight and coerciviness; Dahl, *The Concept of Power*. p.203. He describes the dimensions of base/domain, means/instruments, amount/extent and range/scope.
32 Nye, *The Future of Power*. p.6.; Baldwin, *Power and International Relations*. p.180.; Guzzini, *Structural Power*. p.453.
33 Baldwin, *Power and International Relations*. p.180.
34 Guzzini, *Structural Power*. p.453.
35 Baldwin, *Power and International Relations*. p.180.; Guzzini, *Structural Power: The Limits of Neorealist Power Analysis*, 443-478. pp.453-454.; See also: Dahl, *The Concept of Power*. p.203. He refers to weight simply as the amount or extent an actor has power over another actor.
36 Baldwin, *Power and International Relations*. p.178.
37 Ibid. pp.178-179.
38 Guzzini, *Structural Power*. p.454.
39 David A. Baldwin, *Economic statecraft* (New Jersey: Princeton University Press, 1985). p.149.

in the context of a real or hypothetical situation.[40] In order to determine the context, amongst other, the historical and societal background should be analysed.[41]

2.3 Summary

Although the theoretical foundations of the 'elements of national power approach' and relational power differ with regard to the possession of power and its measurability, the approaches are not irreconcilable. The point of the relational power approach is that a focus on a single or particular set of dimensions could result in tunnel vision, potentially ruling out equally important dimensions. The relational power approach includes the 'means' dimension forwarded by the 'elements of national power approach' proponents, but it adjoins it with other dimensions. As such, the relational power approach is comprehensive. This section will conclude with a framework for analysing power integrating the approaches (see figure 1).

FIGURE 1: POWER ANALYSIS FRAMEWORK. Power manifests itself in a relation between actors; actor A has power to the extent that actor B is receptive to that particular form of power. Whether or not B is receptive depends on a variety of factors, first and foremost the context. Other factors to be taken into account when determining receptiveness are the scope (what is the objective), domain (what actors are involved), weight (likelihood of effectiveness), costs (how costly is the action for A and for B to comply) and means or instruments involved. Barnett and Duvall's concepts of power taxonomy serves to illuminate the power arena of actor's (in)actions and re(in)actions. The power concept utilised in A's (in)action also influences receptiveness and successfulness (compulsory, institutional, structural and/or productive).



3. ASSESSING CYBER POWER

After having discussed the 'old' notion of power, this paper will now reflect on cyber power and its assessment. First, it will define the etymological approach taken to cyber power in this paper, and then sketch the contours of the current cyber power debate by looking at the work of Nye and of Betz and Stevens.

40 David A. Baldwin, 'Power Analysis and World Politics: New Trends Versus Old Tendencies,' *World Politics* 31, no. 2 (1979), 161-194. p.165.

41 Guzzini, *Structural Power*. p.454.

3.1 Cyber power

The meaning of the cyber prefix has undergone some radical changes over time, both in etymological and political senses. Etymologically, it went from being a prefix pertaining to the government element in cybernetics,[42] to a word describing the ethereal world of data,[43] to the contemporary notion in which cyber and cyberspace can be used interchangeably with the Internet, networks and computers. From a security point of view, it went from computer security in the 1960s and 1970s,[44] to information security in the 1980s, resulting in today's coexistence of both information- and cyber-security. From a political viewpoint, cyber went from being a computer threat to critical or vital infrastructure[45] to being both vulnerability and an opportunity to be exploited by intelligence agencies and the military.[46] As a concept of military doctrine it went from being an overarching war fighting concept highlighting the prime role of information on the battlefield,[47] to a current divide over whether or not cyber operations are a subset of information operations.[48]

This paper will take the approach to 'cyber' as pertaining to the intrinsic character of the means and methods used. The specific character lies in its origin, i.e. cyberspace and its specific destination, being other entities within cyberspace. As a result, cyber power would entail conveying power in or through cyberspace. An assessment of cyber power consequently would involve an estimation of an actor's ability to convey power in cyberspace. It can best be understood as: 'the variety of powers that circulate in cyberspace and which shape the experiences of those who act in and through cyberspace'.[49]

Cyberspace refers to the construct created by governmental decision- and policymakers. This is the environment 'formed by physical and non-physical components, characterised by the use of computers and the electro-magnetic spectrum, to store, modify and exchange data using computer networks'.[50] There are more detailed conceptualisations of this domain, which describe various components in cyberspace, namely: geographic, which involves the location; physical, which comprises the network hardware and infrastructure; logical, which captures the software and logical connections; and cyber persona online profiles (such as social-media profiles and mail accounts).[51]

42 See for instance: Norbert Wiener, *The Cybernetics of Society: The Governance of Self and Civilisation* (Cambridge: M.I.T. Press, 1948).

43 See for example: William Gibson, *Neuromancer* (New York: Berkley Publishing Group, 1984).

44 See for instance: Michael Warner, 'Cybersecurity: A Pre-History,' *Intelligence and National Security* 27, no. 5 (2012), 781-799. pp.787.

45 See for instance: The White House, *Securing America's Cyberspace, National Plan for Information Systems Protection: An Invitation to a Dialogue* (Washington, DC: The White House, 2000).

46 See for instance: The Joint Chiefs of Staff, *The National Military Strategy of the United States of America: A Strategy for Today; A Vision for Tomorrow* (Washington, DC: Office of the Chairman, 2004). p.18; The Chairman of The Joint Chiefs Of Staff, *The National Military Strategy for Cyberspace Operations* (Washington, D.C.: Office of the Chairman, 2006). p.3.

47 See for example: John Arquilla and David Ronfeldt, *Networks and Netwars: The Future of Terror, Crime, and Militancy* (Santa Monica: RAND National Defense Research Institute, 2001).

48 See for instance: North Atlantic Treaty Organisation, *Allied Joint Publication 3.10: Allied Joint Doctrine for Information Operations* (Brussels: North Atlantic Treaty Organisation, 2009). pp.1-7 to 1-13.; The Joint Chiefs Of Staff, *Joint Publication 3-12 (R): Cyberspace Operations* (Washington, D.C.: The Joint Chiefs Of Staff, 2013). pp.5-6.

49 Betz and Stevens, *Cyberspace and the State: Toward a Strategy for Cyber-Power.*

50 Michael N. Schmitt, *Tallinn Manual on the International Law Applicable to Cyber Warfare* (Cambridge: Cambridge University Press, 2013). p.258.

51 See for instance: The Joint Chiefs Of Staff, *Joint Publication 3-12 (R): Cyberspace Operations*. pp.I-2 and I-3; United States Army, *Cyberspace Operations Concept Capability Plan 2016 2028* (Fort Eustis: TRADOC, 2010). p.9.

Combining the general notion of cyber power with the more detailed description of cyberspace results in the following notion of cyber power: cyber power comprises the variety of powers affecting the geographic, physical network, logical, and cyber persona components, which consequently shape the experiences of state and non-state actors who act in and through cyberspace. This includes, for instance, using social-media profiles (the cyber persona component) to affect others; the use of offensive cyber means and methods to digitally compromise a critical system (the logical component); or using law enforcement or military powers to physically establish control over network infrastructure (a physical network component).

The proposed notion of cyber power results in all human-induced activities being qualified as cyber power, including routine uses of cyberspace such as emailing colleagues, texting a friend, or posting a Facebook update. This paper will argue that this is indeed cyber power, albeit a very Foucauldian notion of cyber power. Foucault argued that we are moulded and affected by series of discursive power processes, 'power is co-extensive with the social body; there are no spaces of primal liberty between the meshes of the network'.[52]

Every action we take constitutes or is affected by series of social power processes affecting individual decision-making, such as our psyche, subjectivity, personality, consciousness. These power processes influence us constantly, for instance when consuming information (scrolling through social-media timelines only expressing success), responding or not to mails (expressing a power configuration in which the receiver feels obliged to respond promptly or can afford to not respond), and updating social-media profiles (potentially enforcing one's position in a network).

Although it may constitute cyber power, these processes are virtually impossible to unveil and assess. As such, for practically assessing cyber power the scope of Foucauldian cyber power may be too broad and of little use to decision-makers. Adding a form of intentionality would prove much more practical, resulting in cyber power related to the situations in which an actor is *not unintentionally* trying to improve their power position by using cyberspace components. The following section will adjoin this conceptual view of cyber power with more concrete examples.

3.2 Assessing cyber power

How should cyber power be assessed? Betz and Stevens have applied Barnett and Duvall's taxonomy of power concept to analyse cyber power.[53] A similar approach was taken by Joseph Nye who drew on the faces of power discussion and infused it with his hard and soft power theory to analyse power in cyberspace.[54] As a point of departure for assessing cyber power, Nye and Betz & Stevens are more than useful (see table 1).

52 Michel Foucault, *Discipline and Punish: The Birth of the Prison*, 2nd ed. (New York: Random House, 1995).; See also: Digeser, *The Fourth Face of Power*, 977-1007.

53 Betz and Stevens, *Cyberspace and the State*. pp.x-xx.

54 Joseph S. Nye, *Cyber Power* (Cambridge: Harvard Kennedy School Belfer Center for Science and International Affairs, 2010).

TABLE 1: OVERVIEW OF CYBER CAPACITIES TO BE CONSIDERED WHEN ASSESSING CYBER POWER ACCORDING TO NYE, AND BETZ & STEVENS

Joseph Nye's[55] forms of cyber power	Betz and Stevens'[56] forms of cyber power
First face (A induces B to do what B would otherwise not do) *Hard power* • (Distributed) Denial of service attacks • Insertion of malware • SCADA/ICS disruptions • Arrests of bloggers *Soft power* • Information campaigns **Second face (agenda control)** *Hard power* • Firewalls, filters, and pressure to exclude some ideas *Soft power* • Self-monitoring of ISPs and search engines • ICANN rules on domains • Software standards **Third face (preference shaping)** *Hard power* • Threats to punish bloggers *Soft power* • Information to create preference • Develop norms of revulsion	**Compulsory (direct coercion)** • Control of machines or networks • Deploying non-material resources (e.g. threats) **Institutional (via institutions)** • Influence behaviour through institutions • Set norms and standards • Influence foreign audiences via media institutions **Structural (influencing structures)** • Changing structures (e.g. hierarchical to networked) **Productive (constitution of the subject)** • Reproduce and reinforce existing discourses • Construct and disseminate new discourses

Nye earmarks specific means and methods with an effect in cyberspace, and using these would constitute power. The cyber capacities expressed by Nye are almost universal. Whether explicitly or not, every actor has the ability to execute denial of service attacks, issue threats, repress ideas, and conduct information campaigns. Since virtually every actor has these capacities, its use as an analytical tool for policy- and decision makers is doubtful, although it is a very valuable academic insight. A question begging an answer is: how much? How much denial of service, malware insertion and other cyber capacities does one need? And how could one go about assessing how much is required to be successful? Having defined the relational approach to power as leading in this paper, the only logical answer is: it depends on the context and other dimensions of power.

Betz and Stevens have a different, and more conceptual approach to power. As they use Barnett and Duvall's taxonomy of power, they highlight the different processes for conveying power. It is the 'arena' where the battle for power is fought as opposed Nye's description of the potential 'weapons' with which the battle is conducted. As a matter of analysis, Betz and Steven serve the power debate best by showing that Barnett and Duvall's taxonomy can be applied to cyber power. Again, from a policy- and decision making perspective, it adds little to Nye's categorisation.

As discussed above, means alone do not constitute power, and the same goes for the means described by Nye and Betz & Stevens. Stepping into the pitfall of the single-facet approach to power, for instance by only considering the means, would lead to an arbitrary depiction of the

55 Ibid. p.5.
56 Betz and Stevens, *Cyberspace and the State*. pp.45-53.

power situation. The following section will highlight how to assess cyber power by using the power analysis framework depicted in Figure 1.

4. CYBER POWER CONSIDERATIONS

As mentioned somewhat cynically in the introduction, policy- and decision-makers 'relish' comparing their power to that of other actors. Most often, however, this comparison is a dire necessity in the realm of conflict and when considering the viability of a particular course of action. Hence, the practice of comparing power has its value in political and strategic decision-making.

Unfortunately is seems as if we have forgotten the 20th century power debate and start all over when considering cyber capacities. That debate started with the control over resources approach; the actor surpassing the opponent in access to resources was deemed more powerful. We are currently at this stage in assessing the notion of cyber power. We deem the actor with more resources, be they financial, infrastructural, intellectual, or human, to be the more powerful. Although Nye as well as Betz and Stevens use concepts derived from the post-World War II power discussion, the notion lying at heart of their argument is that power can be possessed; the one with the greatest access to resources and means is the most powerful.

This paper deems power to be relational; power manifests itself in a relationship between actors. Whether or actor A is able to influence actor B depends on the context, scope, domain, weight, cost, and means. The following subsections will discuss these dimensions and link them to cyber capacities.

4.1 Context

The context has implications for the effect of an action; the effectiveness of an action depends strongly on the context. The effect of using cyber capacities in the context of a border dispute differs from using them in a trade conflict.[57] There are myriads of contingencies and contexts in which cyber capacities may or may not prove to be effective. Taking heed of the context is essential for analysing the power situation. Any statement on cyber power should be preceded with describing the context of the power use.

4.2 Scope

The scope of an action is about the effect actor A seeks to achieve in actor B; it is about delineating the objective of a certain action. In inter-state affairs there are various objectives sought after at a strategic level, unfortunately, there is no generalised overview of these objectives. As an illustration of potential objectives, this paper will use the strategic objectives, or strategic functions/effects described by the Dutch government, namely: anticipation, prevention, deterrence, protection, intervention, stabilisation, and normalisation.[58]

Taking the scope into account when assessing cyber power is essential as the effectiveness of a particular cyber capability depends greatly on the objective sought. Some capacities are better

57 Baldwin, P*ower Analysis and World Politics*. p.164.
58 Ministry of Defence (Netherlands), *Future Policy Survey: Summary and Conclusions* (The Hague: MoD, 2010). pp.14-15.

suited for achieving a specific objective than others. For example, a state-owned or bought botnet may serve as a deterrent – that is, if their existence is disclosed – but may have very little effect in stabilising another country. The same goes for disclosing information regarding state-owned, bought, or distributed malware;[59] budget increases in the realm of cyber capacities;[60] or a speech dissuading any potential adversary from impinging on state affairs.[61] These may have deterrent, preventative, or protective effects, but they will lack effectiveness in achieving normalisation or stabilisation of a situation. The use of communication channels on the Internet such as social-media (Twitter, Facebook, YouTube) and other media (instant messaging, 'regular' messaging) may contribute to stability and normalisation in a region,[62] although they may lack a deterrent effect. The scope of the action and its objectives influence whether or not actor A can effectively influence actor B.

4.3 Domain

Domain 'refers to the […] actors subject to [the] influence [attempt]'[63] or simply 'the target[s]'.[64] It is about the type and number of actors influenced by actor A. The domain is crucial to assess power, as the effectiveness of a particular action depends greatly on who actor B is, and how many B's there are. Depending on the domain, or the targets, taking a particular course of action may or may not be effective. Cultural, political and many other aspects of actor B may render it unreceptive to influence exerted by actor A. For instance, a state with strict media controls or censorship in the physical and virtual domain may be unreceptive to inputs from actor A in the realm of social and conventional media. Also, if the domain comprises more than one actor, this will have an impact on the potential effectiveness of actor A's influence attempt. The target actors may differ in preference or location, possibly making it harder for actor A to effectively influence them, and so the nature and number of actor B will greatly influence the effectiveness of a particular course of action undertaken by A.

4.4 Weight

The weight relates to the (potential) effectiveness of power; that is, the likelihood that 'B's behaviour is or could be affected by A'.[65] The actor who has a higher chance of achieving its objectives (weight) can be considered, in a specific context, to be more powerful. The weight of an actor's action depends on all other power dimensions. As such, it may be perceived as the sum of all dimensions and an indicator to who is powerful in a given situation.

4.5 Costs

Costs indicate both the cost to actor A and the costs to B; 'is it costly or cheap for A to influence

59 'Special Report: U.S. Cyberwar Strategy Stokes Fear of Blowback,' Reuters, last modified May 10, accessed December 23, 2015, reuters.com/article/usa-cyberweapons-idINDEE9490AX20130510.

60 See for instance: 'Cyber Command's Exploding Budget,' The Washington Post, last modified January 15, accessed December 23, 2015, washingtonpost.com/news/the-switch/wp/2014/01/15/cyber-commands-exploding-budget-in-1-chart/.

61 See for example: 'U.S. Decides to Retaliate Against China's Hacking,' The New York Times, last modified July 31, accessed December 23, 2015, nytimes.com/2015/08/01/world/asia/us-decides-to-retaliate-against-chinas-hacking.html?_r=0.

62 See for instance, community policing via social-media: 'Kenyan Chief's Twitter Feed Helps Round Up Stolen Cows and Lost Phones,' Los Angeles Times, last modified September 1, accessed December 23, 2015, latimes.com/world/great-reads/la-fg-c1-kenya-twitter-20150901-story.html.

63 Baldwin, *Power and International Relations*. p.180.

64 Guzzini, *Structural Power*. p.453.

65 Baldwin, *Power and International Relations*. p.180; Dahl, *The Concept of Power*. p.203. He refers to weight simply as the amount or extent an actor has power over another actor.

B? Is it costly or cheap for B to comply with A's demands?'[66] These costs for A and B are indicative of power, and 'some have suggested that more power should be attributed to an actor that can exercise influence cheaply'.[67] For example, if it is cheaper for A to influence than for B, actor A is deemed more powerful. Or when A can cheaply influence B to do something costly, A is considered more powerful. In the realm of cyber capacities, costs are an interesting dimension to power. Some capacities are very asymmetric, that is, low cost and high return. For instance a distributed denial of service attack costs very little,[68] and can cause great financial damage[69] by necessitating DDoS mitigation and forensic services, and the financial loss due to the inability to conduct business. Not only a low level attack such as a DDoS is asymmetrical, even a high-end, costly, multi-year intrusion operation like Stuxnet, Flame or Duqu may cause more damage in financial, political, or symbolic senses than its development cost. In other words, costs should be weighted against the benefits or effects of the action.

4.6 Means

Means refer to the various instruments of exercising influence, and there are many ways to categorise such means. Various authors have forwarded categorisations of instruments of state power or statecraft. Military scholarly research often uses the diplomacy, informational, military, and economic (DIME) categorisation, a concept spawned during the Cold War.[70] In the post 9/11 decade, financial, intelligence, law enforcement and 'other civil capacities' instruments were added, resulting in the DIMEFIL or MIDLIFE acronym.[71] There are many other categorisations rivalling or, sometimes, dwarfing the DIMEFIL construct in comprehensiveness and academic stature. This subsection will first briefly discuss the instruments of state power, and then forward an overview of the means enclosed in the DIME, DIMEFIL and other categorisations. After that, these means will be supplemented with cyber capacities described by Nye and Betz & Stevens, and other cyber capacities.

Although the instruments of state power are not subject to much debate, the 'terminology in this domain is not widely agreed upon'.[72] Carr's 1939 *The Twenty-Years' Crisis* serves as the starting point for most writings on instruments of state power. Carr divided political power, 'for the purpose of discussion',[73] into three categories: '(a) military power, (b) economic power [and] (c) power over opinion'.[74] Carr's categorisation of political power was significantly influenced

66 Baldwin, *Power and International Relations*. p.178.
67 Ibid. p.178.
68 See for instance: 'How Much does a Botnet Cost?' Threatpost, last modified February 28, accessed December 25, 2015, threatpost.com/how-much-does-botnet-cost-022813/77573/.
69 'Collateral Damage: 26% of DDoS Attacks Lead to Data Loss,' Kaspersky, last modified September 17, accessed December 25, 2015, kaspersky.com/about/news/business/2015/Collateral-damage-26-per-cent-of-DDoS-attacks-lead-to-data-loss.
70 Joint Chiefs of Staff, *Joint Publication 1: Doctrine for the Armed Forces of the United States* (Washington, DC: Joint Chiefs of Staff, 2013).; Ministry of Defence, *Joint Doctrine Publication 0-01: British Defence Doctrine*, 4th ed. (Shrivenham: Development, Concepts and Doctrine Centre, 2011).; Dutch Ministry of Defence, *Netherlands Defence Doctrine* (Den Haag: Ministerie van Defensie, 2013).; North Atlantic Treaty Organisation, *Allied Joint Publication 1(D): Allied Joint Doctrine* (Brussels: Nato Standardization Agency, 2010).
71 'The National Security Strategy of the United States of America,' , state.gov/documents/organisation/63562.pdf. Preface; Dutch Ministry of Defence, *Netherlands Defence Doctrine*. p.22.; Robert D. Worley, *Orchestrating the Instruments of Power: A Critical Examination of the U.S. National Security System* (Raleigh: Lulu Press, 2012). p.181.
72 Worley, *Orchestrating the Instruments of Power*. p.181.
73 Edward H. Carr, *The Twenty Years' Crisis 1919-1939: An Introduction to the Study of International Relations*, 2nd ed. (London: MacMillan & Co. Ltd., 1946). p.108.
74 Ibid.

by the *interbellum*;[75] hence parts of his categorisation may seem out-dated as he pointed out himself in the preface to the second edition. Michael Mann has forwarded a more modern approach to sources or instruments of power, namely the IEMP-model, short for ideological, economic, military, and political power sources.[76] Carr's and Mann's categorisations have been widely used and discussed in academia, but are not employed by those using the instruments or those constituting the instruments.

Although there are semantic differences between Carr, Mann and the governmental categorisations, the instruments have considerable overlaps and can be summarised as:

- the political instrument, comprising internal politics and outward facing diplomacy;
- the informational instrument, aimed at spreading, collecting, protecting and monitoring information;
- the economic instrument, comprising the use of finance and economic statecraft to influence other actors;
- the military instrument, serving as an extension of foreign policy both coercively (hard power) and attractively (soft power); and
- other (civil) capacities such as legal power, law enforcement, administrative organisations, education, healthcare, utility companies, etc.

TABLE 2: OVERVIEW OF THE INSTRUMENTS OF STATE POWER AS DESCRIBED BY CARR, MANN AND DIME(FIL) PROPONENTS, THE MEANS THESE INSTRUMENTS DESCRIBED BY VARIOUS AUTHORS AND THEIR CYBERSPACE EQUIVALENT

Instrument	Capacities	Cyber capacities
Political	• Wield other instruments (Carr) • Internal politics (Mann) • Geopolitical diplomacy (Mann) • Achieving foreign policy objectives (DIME)	• Coordination (e.g. command and control systems) • Legitimise actions via social-media • Use cyber capacities as deterrent (e.g. 0days, malware, strike-back) • Use cyber capacities to intervene abroad (e.g. Stuxnet, Orchard)
Informational	• Gain power over opinion (Carr) • Unify meaning, norms and aesthetic and ritual practices (Mann) • Controlled release of information (DIME) • Protecting own information (DIME) • Collecting information (DIMEFIL)	• Manipulate internal and external target audiences (e.g. social-media) • Shape target audiences via information campaigns (e.g. troll-army tactics) • Legitimise own and delegitimise foreign actions via (social-)media • Use cyber capacities aimed at defence (e.g. IDS, IPS, etc.) • Use cyber capacities aimed at intelligence (e.g. surveillance)
Economical	• Gain autarky or influence abroad (Carr) • Monopolise control over classes (Mann) • Support or combat other actors (DIME) • Disrupt finance of other actors (DIMEFIL)	• Protect own industries or gather competitive intelligence. • Nationalise control over Internet infrastructure/security • Support actors financially or materially (e.g. network infrastructure) • Disrupt financial traffic (e.g. SWIFT)

75 Ibid. Preface to the second edition.

76 Michael Mann, *The Sources of Social Power: A History of Power from the Beginning to A.D. 1760*, Vol. I (Cambridge: Cambridge University Press, 1986).; Michael Mann, *The Sources of Social Power: The Rise of Classes and Nation-States 1760-1914*, Vol. II (Cambridge: Cambridge University Press, 1993).; Michael Mann, *The Sources of Social Power: Global Empires and Revolution 1890-1945*, Vol. III (Cambridge: Cambridge University Press, 2012).; Michael Mann, *The Sources of Social Power: Globalisations 1945-2011*, Vol. IV (Cambridge: Cambridge University Press, 2013a).; Michael Mann, 'The Sources of My Sources,' *Contemporary Sociology: A Journal of Reviews* 42, no. 4 (2013b), 499-502.

Instrument	Capacities	Cyber capacities
Military	• Extending foreign policy (Carr) • Intensive power over limited space (Mann) • Extensive power over larger space (Mann) • Hard coercive power (DIME) • Soft attractive power (DIME)	• Intervene or stabilise abroad via military cyber capacities • Establish control over infrastructure (e.g. tailored access) • Influence actors via deterrence (e.g. a show of force in cyberspace) • Deny, disrupt, degrade, destroy infrastructure (e.g. DDoS, malware) • Information campaigns aimed at target audience (e.g. via social-media)
Other capacities	• Legal power (DIME) • Law enforcement (DIMEFIL) • Administrative organisations (DIME) • Education (DIME) • Healthcare (DIME) • Utility companies (DIME)	• Prosecuting bloggers/hackers • Arresting and detaining bloggers/hackers • Influence institutions (ICANN, ISPs, etc.) • Provide cyber awareness courses, stimulate computer sciences, etc. • Protect or deny infrastructure to opposing actors • Ibid.

Table 2 shows that most instruments have a cyber aspect to them, and that the instruments of state power extend into cyberspace. Unlike Nye, Betz and Stevens, this paper will not categorise these means under the faces of power or the taxonomy of power. The reason for not using these categorisations is that cyber capacities can be used for a wide variety of purposes, and using these categorisations could foster the thought that certain capacities can only be used for one specific purpose. That would deny the universal application of the instruments of state power and cyber capacities. All the instruments can be used to gain state objectives, military power can achieve political objectives, economic power can achieve military objectives, and (civil) capacities can attain informational objectives.

All the cyber capacities can be used for attaining any of these objectives. For instance, a DDoS aimed at a foreign military can also be used to DDoS a financial institution. Cyber capacities can exert influence via a myriad of power mechanisms, hard and soft, compulsory institutional, structural, and productive. The instruments of state power involved and their extension in cyberspace affect the effectiveness of actor A influencing actor B.

5. CONCLUSION

This paper's purpose was threefold, providing: (1) a basis for further discussion about cyber power; (2) footholds for assessing cyber power; and (3) a viewpoint on the categorisation of cyber capacities within the power debate.

Section 2 provided a brief, albeit theory-laden, overview of the 20th century power discussion. This paper, taking a relational approach to power, tried to emphasise the other dimensions of power, being: scope, domain, weight, costs, and means. Figure 1 incorporates these dimensions and mechanisms for conveying power (compulsory, institutional, structural, and productive) into a model for analysing power.

Section 3 drew the outlines of the current cyber power debate by first defining cyber power and secondly sketching the views promoted by Nye and by Betz and Stevens in their work regarding cyber power. The means they describe are very useful to anyone looking to assess cyber power, however, they have to be considered alongside the other power dimensions.

Section 4 adjoined the power analysis framework in section two with contemporary notions regarding cyber power and capacities. Any appreciation of cyber power should include the context (what is the context?); scope (what is actor A trying to achieve); domain (what actors and type of actors are involved?); weight (how likely is actor A in successfully influencing actor B?); costs (how costly is the (in)action taken by actor A and how costly is it for actor B to comply?); and means (what instruments of state power and their cyber equivalents are involved?).

To the disappointment of many policy- and decision-makers, this paper will not present a generalised overview of the powerful and the powerless actors on the world stage. The reason for not doing so is that any such statement would be flawed. A generalised overview of cyber power distribution cannot exist because it depends on all dimensions of power. As all these dimensions are contextual and some are temporal; there are too many contingencies to be captured in such an overview. This is not unique to cyber power, since the start of discussions about power it has been shown to be notoriously hard to capture in qualitative and quantitative terms.

That does not mean, however, that an appreciation of cyber power distribution is without use. An overview of the cyber power distribution, for instance by looking at the means (e.g. network infrastructure, spending, government wide cyber security budgets, acquiring malware, DDoS capacity, IT-graduates, etc.), can offer insights to policy- and decision-makers. It is, however, paramount to realise that these results have to be interpreted in their context and adjoined with the other dimensions of power. The power analysis framework forwarded in this paper can be used to that extent.