The Digital Divide: A National Security Argumentative Analysis within a South African Context

Jackie Phahlamohlaka[1], Mapule Modise[1], Nthumeni Nengovhela[2]
[1] Council for Scientific and Industrial Research, Pretoria, South Africa
jphahlamohlaka@csir.co.za
mmodise@csir.co.za

[2] Defence Secretariat, Department of Defence, Pretoria, South Africa
nthumeni@gmail.com

Abstract: Since it was coined in the early eighties following the Maitland commission for worldwide telecommunications development, much has been written about the concept of digital divide. Everything to date in the literature about the subject point to its complexity and dynamism, resulting in efforts aimed at closing the divide contributing to widening it. It is a problem with properties of insolvability. Our aim in this paper is to illustrate that there is value in drawing from these arguments in order to stimulate scholarly debate and possible illumination of National Security issues within a South African context. We do this by following a Hegelian dialectical approach, with our illustration and argument organised in accordance with the determinants of national power.

Keywords: Digital Divide, National Power, National Security, Security threats, Hegelian Dialectic.

1. Introduction

Technological advances in Information and Communication Technologies (ICTs) is seen by many commentators as underpinning the social and economic progression of nation states throughout the first stages of 21st century [8]. To an academic, the developments in ICT "offer an unprecedented opportunity to overcome existing social division and inequalities" [8], to the politician these developments are seen as "the indispensable grammar of modern life and fundamental aspects of citizenship in the prevailing information age". As a result of these changes, information is now regarded as a major determinant of national power which is the cornerstone of National Security.

In the midst of these zealousness and over-enthusiasm over developments in ICT, concerns about the divisive aspect of the information age grew. It was issues of inequalities of access to both information and technology that gave rise to the emergence of a digital divide "phenomenon". Narrowly, digital divide was seen as the divide between *the haves and have-nots* and a vast body of literature produced, focused on the existence of this gap and how to bridge it. Within the South African context, there are very conspicuous and acknowledged contradictions. The gap between *the haves and the have-nots* is the largest in the world, while at the same time there is an Act of parliament, the Universal Services Act of 1996 that declares access to ICT as a basic human right. Everything to date in the literature about the digital divide point to its complexity and dynamism, resulting in efforts aimed at closing the divide contributing to widening it.

Our aim in this paper is to illustrate that there is value in drawing from the digital divide arguments in order to stimulate scholarly debate and possible illumination of National Security issues within the South African context. We do this by following a Hegelian dialectical approach [2], with our illustration and argument organised in accordance with the determinants of national power. From two authoritative sources, the United Nations Department of Economic and Social Affairs [10] and the Internet World Statistics [3]; we draw five mostly argued dimensions of the digital divide against which identified National Security threats are contrasted. It is the synthesis from these contrasts that we believe illuminates some of the National Security issues from within the South African context. The paper adopts an analytical argumentative approach that addresses the following key question:

In what ways do the arguments about the digital divide contribute to a better understanding of National Security issues within a South African context?

In addressing the above question, the paper is structured as follows: the next section presents brief definitions of the digital divide and National Security. This is followed by an analysis of the digital divide framed within the determinants of national power as embedded in the National Security definition. It is within this analysis that the five mostly argued dimensions of the digital divide are contrasted against identified National Security threats. The five mostly argued dimensions of the digital divide are distilled from two major sources, the United Nations Department of Economic and Social Affairs [10] and the Internet World Statistics [3]. The identified security threats we use are those presented by Jansen van Vuuren *et al* [5].

2. Definition of Key Concepts

2.1 The Digital Divide

The term has been used loosely although fundamentally to illustrate the gap between those who have meaningful access to digital information through different information resources and those without access at all. The primary divide is the access to ICTs while the secondary divide being the ability to use those technologies effectively in order to yield results of participating in the global world.

Digital divide of yesterday referred and focused on access to infrastructure while digital divide of today refers to the disparities between the information rich and information poor. The missing link was more concentrated on the infrastructure disparity, and was solved by just installing the telephone lines. No education or literacy training was required to use the capability while today's divide is more complex. The new technologies (internet, etc.) require some level of education in order to bridge the gap effectively. Drawing from different definitions, stated above and in perspective with the above-mentioned challenges, this paper defines digital divide as the gap between those who have access to ICT resources and the ability to use them in comparison to those who do not have. The assumption being that those who effectively use ICTs are participants in the digital and information economy.

2.2 A perspective on National Security

The literature indicates that there are as many definitions of National Security as there are students. One definition that is mostly used is the one given by David Jablonsky [4], who defines National Security as that part of government policy whose objective is to create national and international political conditions that are favourable to the protection or the extension of vital national values against existing or potential adversaries.

According to Jablonsky, National Security is defined in terms of the respective elements of the power base of a state, and is allotted differing priorities within different states, depending on the declared vital and national interests of such a state. All definitions of National Security include the concept of national power, without which it is argued, there can be no security. The elements of national power fall into either of the two categories of determinants of power. The natural determinants and the social determinants. The natural determinants (geography, resources, and population) are concerned with the number of people in a nation and with their physical environment. Social determinants (economic, political, military, psychological, and informational) on the other hand concern the ways in which the people of a nation organise themselves and the manner in which they alter their environment [4].

What Jablonsky does not focus on though, is the concept of human security as part of National Security. Within the South Africa context, human security is not only a legal issue as articulated in the White Paper on Defence of 1996, it is a constitutional principle, at whose core is the security of people, and not so much that of the state. The first governing principle, principle 98 of the South African Constitution state very clearly that "National Security must reflect the resolve of South Africans as individuals and as a nation, to live as equals, to live in peace and harmony, to be free from fear and want, and to seek a better life" [1].

From the literature, one can define 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 [6]. To understand National Security, one must understand the elements of national power and how they interrelate.

3. The Digital Divide and the Determinants of National Power

In this section we perform an analysis of the digital divide framed within the determinants of national power as embedded in the National Security definition. It is within this analysis that the five mostly argued dimensions of the digital divide are contrasted against identified National Security threats. The five mostly argued dimensions of the digital divide are distilled from two major sources, the United Nations Department of Economic and Social Affairs [10] and the Internet World Statistics [3]. The identified security threats we use are those presented by Jansen van Vuuren *et al* [5] in their recent paper presented at the International Conference in Information Warfare and Security. While the five mostly argued digital divide dimensions are drawn from global studies, the identified National Security threats were largely in relation to the African situation, with a focus on the South African situation.

A brief description of these dimensions follow:

Economic equality
Some think that access to the Internet is a basic component of civil life that some developed countries aim to guarantee for their citizens. Telephone is often considered important for security reasons. Health, criminal, and other types of emergencies might indeed be handled better if the person in trouble has an access to the telephone. Another important fact seems to be that much vital information for people's career, civic life, safety, etc. are increasingly provided via the Internet. Even social welfare services are sometimes administered and offered electronically.

Social mobility
Some believe that computer and computer networks play an increasingly important role in their learning and career, so that education should include that of computing and use of the Internet. Without such offerings, the existing digital divide works unfairly to the children in the lower socio economic status. In order to provide equal opportunities, governments might offer some form of support.

Democracy
Some think that the use of the Internet would lead to a healthier democracy in one way or another. Among the most ambitious visions are that of increased public participation in elections and decision making processes.

Economic growth
Some think that the development of information infrastructure and active use of it would be a shortcut to economic growth for less developed nations. Information technologies in general tend to be associated with productivity improvements. The exploitation of the latest technologies may give industries of certain countries a competitive advantage.

Achieve other development goals
In most of the existing literature, it is argued that having access to information is essential to achieve other development goals, meaning that by overcoming the obstacles to bridge the digital divide, societies will become more productive and integrated with each other, thus reducing development problems.

We are now ready for our National Security argumentative analysis using the above five arguments and contrasting them against the identified security threats framed within the determinants of national power. It is a point (*digital divide dimension*) – counterpoint (identified security threats) analysis. Within each of the eight determinants of national power, we start by presenting the digital divide dimension (point), followed by the identified security threats (counter point). The digital divide dimensions are in *Italic.*

3.1 Natural determinant analysis

3.1.1 Geography and resources

In most of the existing literature, it is argued that ICT serves as a medium that closes the distances between populations that are rural and remote. By overcoming the distance obstacles through ICTs, provides access to information and communication and breaks down the barriers to knowledge and participation, thus creating societies that are productive and integrated with each other. [7]

As an attempt to give access to all, Africa has approximately 100 million PCs, of which 80% are infected with some kind of malware - compared to 30% in the UK. The shipment of outdated PCs to Africa also pose a security threat to the continent as old and outdated software is very vulnerable to attacks because security updates are not available anymore. Wuest of Semantic Labs predicted that the increased access to broadband will result in internet users being attacked up to a thousand times a day, while larger websites can experience up to one million attacks per day" [5].

While the African region's concerns are justifiably to remove the barriers to access and utilisation of ICTs, there are inherently and often overlooked security threats. For instance, an increased internet access, goes with an increased vulnerabilities, infections and malware. With less knowledge and resources to protect the Internet users against potential attacks, it could be argued that from the National Security point of view, the tone for the call to increased access should be taken with a pinch of salt. A properly managed access preceded by an intensive awareness campaign on the possible negative effects could, in the long run, yield the desired result.

3.1.2 Population

There is a view in digital divide discourse that lack of access and use of technology restrict learning opportunities and thus impedes social mobility. This, it is argued, have direct links to developmental issues of poverty and unemployment.

"In the past year, the Internet user base in South Africa has seen its highest rate of growth since 2001, increasing by 12.5% to 4,5-million. There are currently 67 million internet users in Africa… The new broadband access could see millions of new users connecting to the Internet via unprotected devices. … Naxal watch state that if PCs can be related to people and if every infected PC were a person this can be the worst pandemic in the history of the word." [5]

There exist a correlation between the internet technology penetration rates and education such that the internet's content is created by and for the more highly educated. Given the fact that Africa is characterised by high levels of illiteracy, one can argue that since access to technology is often readily available to those in a higher socioeconomic group, inequitably access creates societal polarisation. Again, more connectivity means more computers in the hands of unsuspecting and perhaps not so sophisticated users. This could pose serious threats to National Security of any country as the compromised computers could be remotely controlled to launch attacks from anywhere in the world.

3.2 Social determinants

3.2.1 Economical

There is a notion that ICTs should lead to positive economic outcomes by making markets more transparent through greater access to information, and more efficient through the resulting decline in transaction costs [11].

"… Although access to broadband is still very low in South Africa it did not prevent hackers to con the public in South Africa to reveal their vital personnel information. … The problem resulted in payments debited against customer's accounts not transferred to vendors. Bank serve handles 2.5bn transactions worth R8tm per year. If an attack were to happen, business to business transactions would be impossible, nobody will be able to use ATM and in addition no salaries will be paid, except by resorting to manual system" [5].

Commercial, social, educational and other types of essential services could undeniably be speeded up with increased connectivity. Compared to the extent of the economic damages being witnessed recently, coupled with the fact that these damages are mostly not subjected to public scrutiny, it is argued that adverse economic issues facilitated and speeded by increased internet connectivity if not sufficiently addressed could pose serious threats to the security of any nation.

3.2.2 Political

Support for democracy in the digital divide literature is an important political issue. Increased public participation in elections and decision making processes could be made easier by increased access to the internet. ICTs assist governments and agencies in reaching the "unreached" and through many programs alleviate poverty in rural and remote areas. It also enables the involvement and empowerment of the marginalised and ensures their participation in the governance process.

"There have been increases in reports received of cyber attacks and network infiltrations that appear to be linked to national states and political goals. .. Cyber attacks with political connotation were seen in Estonia, Georgia and South Korea in the last few years. … The Congress of South African Trade Unions (COSATU), the African National Congress (ANC) alliance partner, had been victims of such an attempt when a scam email was send with the information that they will soon embark on a nationwide strike. This followed a recent attack on the ANC's website where the party was embarrassed when pornographic advertisements appeared on their website" [5].

There are many very good examples where ICTs are used to support democracy and increased public participation in political processes. The use of social networking tools during the last US elections is the case in point. From a National Security point of view though, the same tools could be used to cause major political upsets. Cyber attacks on a country's critical infrastructure as well as disruption of essential services have been demonstrated in Estonia, Georgia and South Korea. Scams aimed at discrediting political parties have recently also been observed in South Africa and Zimbabwe, with websites of ruling parties being attacked. Groups claiming to be acting on behalf of the Afrikaner community [9] are also using social networking media to lobby support for their political ideals.

3.2.3 Military

Digital divide can be used as a measure of how vulnerable the state has become. The decline in military spending by many states had paved a way to balance the social and economic developments of many states. In Africa, the outcomes do not show this tendency. The move from conventional warfare to digital warfare or currently well known as the network centric warfare is a fantasy to the African region.

".. Militaries are also considering using cyber attacks on their enemies. Denial-of-service (DOS) attacks were initiated by Russian civilians and sympathisers in coordination with the Russian military and organised crime were scheduled to be synchronised with the invasion of the Russian military into the former Soviet state. .. These cyber opportunities and threats will result in moving the war to the civilians' households using their personal PCs. Compromised armies of machines could be used to launch attacks on the enemies' infrastructure with or without the knowledge of government or the military" [5].

The fact that South Africa and Africa in general is less connected is perhaps an advantage from a military perspective of national power. South Africa is a regional power, and despite the low penetration of internet connectivity, it still has a high risk of becoming a victim of cyber war. Also, some of the disgruntled civilian groupings could easily turn themselves into 'cyber warriors', posing a threat to National Security.

3.2.4 Psychological

There are arguments in the digital divide literature that attention should be paid to social, cultural and psychological factors that may limit Internet use to a level well below the almost complete level of saturation achieved by television.

“The Georgian attack done by supporters and civilians can be seen as a relatively decent example of cyber warfare combining PSYOPs (psychological operations) and self-mobilisation of the local Internet users by spreading “For our motherland, brothers!” or “Your country is calling you!” hacktivist messages across web forums. The attackers defaced the presidential website, and while keeping up the DDoS attack, played an integrated slide show portraying President Saakashvili next to Hitler, with identical images of both Saakashvili and Hitler’s public appearances” [5].

Two interesting but very pertinent questions could be asked here, 1) What if the internet had reached the same level of penetration as television? 2) What if all groupings in South Africa had equal access to the internet and were able to maximise the use thereof to perform psychological types of operations to lobby for the support of their course? Our take is that there would probably be more work for the National Security agencies of the country to focus on human security of its citizens, protecting them from the possible psychological onslaughts as the internet is not as visible and easily regulated as the television.

3.2.5 Informational

South Africa identified the need for ICT access to all its citizens as indicated in the Draft Broadband Policy of September 2009. This must be promoted on all levels of the community and everybody must be exposed to the use and benefits of ICT. In addition to the Broadband policy, South Africa has two Acts of Parliament, the Universal Services Act of 1996 and the Promotion of Access to Information Act of 2000; both of which declares access to information as a basic human right within the South African context.

“With increased broadband access and connectivity by all its citizens go the possibilities of malicious code that could overwrite the infected PC’s hard drive which could result in massive loss of data and information. Attacks with similar malware, used in the cyber attack on the US and Korean government and commercial Web sites in 2009, can have serious impact on service delivery and information required by the citizens. If these malicious codes include instructions that will overwrite the PC’s infected hard drives, it will spell out disaster for many tens of thousands of PCs. Citizens, communities and businesses would be severely affected in this process” [5].

Information is certainly regarded as a major determinant of national power. As Dan Kuehl points out, where the greatest improvement is required in information operations is in the development of information ‘strategists’; those who are able to coordinate and exploit the contribution of the information component of power and synergies it offers to the other elements of national power. While there are two Acts of parliament in South Africa to emphasise this point, it is perhaps the lack of these information ‘strategists’ that make their conversion to vehicles that could better the quality of lives of South Africans a difficult task.

4. Conclusion

From this synthesis performed by contrasting the digital divide dimensions and the identified security threats accompanying broadband access using the determinants of national power, we believe we have achieved the aim of the paper. We believe that the dialectical arguments together with the synthesis structure provided in this paper, provides the reader with an opportunity to think differently about the digital divide particularly from a National Security perspective. Whereas the digital divide debate has recognised the interconnectedness of technology access to social factors, uneven development, and global capitalism, it still fails to map all these into the National Security debate. As a result, we conclude that any debate on the digital divide that does not take into account the National Security issues remains incomplete. It is our view that by following the digital divide arguments, we have shown how some pertinent National Security questions could be explored, thus enhancing the understanding of its complexity within the South African context.

References

[1] Constitution of the Republic of South Africa, Chapter 11, Governing Principle 198, pp 112, 1996.

[2]Hegelian Dialectic definition, accessed 20100628, Available online at http://en.wikipedia.org/wiki/Hegelian_Dialectic.

[3]Internet World Statistics, accessed 20100628, Available online at http://www.internetworldstats.com/links10.htm.

[4] D. Jablonsky, D. "National Power", In Cerami, J.R., Holcomb, J.F, Jr. (eds). U.S. Army war college guide to strategy, 2001, also available online at http://www.au.af.mil/au/awc/awcgate/army-usawc/strategy2004/index.htm.

[5] J. Jansen van Vuuren, L.J Phahlamohlaka, M. Brazzoli, "The Impact of the Increase in Broadband Access on South African National Security and the Average Citizen", in proceedings of the 5th International Conference in Information Warfare and Security, Air Force Base Institute of Technology, Ohio, Dayton, USA, pp. 171-181, 2010.

[6] J. Phahlamohlaka, "Globalisation and National Security Issues for the State: Implications for national ICT Policies", In IFIP International Federation for Information Processing, Volume 282, Social Dimensions of Information and Communication Technology Policy, Chrisanthi Avgerou, Matthew L. Smith, Peter van Besselaar, (Boston Springer), pp 95 – 107.

[7] D. Roode, H. Speight, M. Pollock, R. Webber, "It's not the digital divide – It's the socio-techno divide", in proceedings of the European Conference in Information Systems (ECIS 2004).

[8] N. Selwyn, Reconsidering Political and Popular Understanding of the Digital divide, accessed 20100627, Available online at http://nms.sagepub.com/cgi/content/abstract/6/3/341.

[9] Social networking use for political lobbying, "South Africa Sucs", accessed 20100628, Available online at http://boerboel1.wordpress.com/2010/05/23/the-ancnaspers-psyops-against-the-afrikaner/.

[10] United Nations Department of Economic and Social Affairs, accessed 20100627, Available online at http://www.globalenvision.org/library/7/1406.

[11] Http://wiki.media-culture.org.au/index.php/Digital_Divide#Debate_over_the_Digital_Divide