National security governance exemplified by South Africa's cyber security policy implementation

Oliver K. Burmeister (School of Computing and Mathematics, Charles Sturt University, Australia), Jackie Phahlamohlaka (Defence, Peace, Safety and Security, CSIR, South Africa), and Yeslam Al-Saggaf (School of Computing and Mathematics, Charles Sturt University, Australia)

Abstract

There exists a paucity of research on ethical considerations in cyberdefence policies that can provide nation states guidance in mitigating the risks of a cyber attack to their national interests and to preparing for a cyber offence in response to an attack. A discourse analysis of the "0x Omar"-Israeli conflict of 2012, as reported in the Arabic and English media and on the Internet, is used to explore ethical issues that this case raises and to examine how the risks posed could be mitigated in relation to relevant elements of the South African cybersecurity policy framework. Questions raised include: At what point does the policy require a nation state to prepare for a cyber offence in response to a cyber attack?; and, How does a nation determine if the attack is directed towards a particular company, or against the nation?

1. Introduction

Cyberdefence raises several ethical issues including the 'attribution problem', moral responsibility, the inadequacy of secure systems, and the moral justification of a cyber attack on a nation state's vital interests in response to a cyber attack carried out by people residing in that nation state. Yet, research on these ethical issues is scarce. Such research is needed to assist nation states in mitigating the risks of a cyber attack to national interests.

While the 'attribution problem', the moral responsibility of nation states, as opposed to that of individuals within a nation state, and the moral justification of a cyber attack are still debated, cyber attacks continue to pose real threats. Those threats need to be recognised when they occur and responded to immediately, to protect sensitive infrastructure, as well as individual citizens. Governance of security policies could ensure that national interests are safe-guarded, that peaceful solutions to threats are effected, and that where necessary, counter-measures are successfully implemented.

Using a discourse analysis of the "0x Omar"-Israeli conflict of 2012, as reported in the Arabic and English media and on the Internet, this article explores the ethical issues. It examines how the risks posed could be mitigated through policy implementation. The "0x Omar"-Israeli conflict of 2012 revealed multiple areas that a nation needs to safe-guard against. Initially it appeared an isolated incident, then it appeared to be a coordinated attack against national infrastructure. Deception was involved not only in the strategy employed to make it appear isolated initially, but also in terms of who the attackers were. At first it was not clear if it was the work of an isolated terrorist, or something more sinister. Even when it became clear that the nation initially thought

responsible for the attack was not responsible, and there was strong evidence that it was another nation, that evidence was inconclusive for some time.

This article begins with a review of national security within the context of cyber attacks. It examines how policies have been developed to mitigate the threats posed by such attacks, and goes on to examine the case allegedly involving "0x Omar" and Israel. Then an analysis of relevant elements of the South African cybersecurity policy framework is conducted in relation to ethical dimensions of the "0x Omar"-Israeli case. Finally implications are drawn for other national security policies.

2. Literature Review

Cyberdefence has grown in scope over recent decades, particularly as nations have taken steps to provide wider segments of their society with access to information infrastructure. There have been numerous instances of attacks on national infrastructure, such as the well publicised attacks on Estonia (Shackelford, 2009). As nations expand their national broadband capabilities, they become more attractive targets to cyber attacks (Phahlamohlaka, Modise, & Nengovhela, 2008; Phahlamohlaka, van Vuuren, & Coetzee, 2011). Three areas define what is encompassed by the terms 'national security' and 'cyberwar', as well as showing how policies could act as mitigation strategies.

2.1. National security involving ICT

Security is an important concern of national governance. Shackelford (2008) distinguishes national and international security, in his discussion of 'net war' and cyber attacks, and international law. Where Shackelford argued that the best way to combat cyber attacks is through revisions to international laws and treaties, our focus is upon the responsibilities of nation states to enact policies that protect their citizens from cyber attacks that are against the national interest. However, Phahlamohlaka (2010, p. 103) claimed that national borders are becoming irrelevant and that information and communications technologies (ICT) removes the differentiation between international and domestic threats. Similarly, Jablonsky (2002) indicated that the distinctions of national and international security tend to blur when discussing cyber security. Jablonsky defined 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.

Historically the concept of 'national security' has been associated with the, post World War II, US Congress passing of the first National Security Constitution in 1947. This defined national security as "to do with the protection of the state against external aggression through economic, military, political, and diplomatic means" (Phahlamohlaka, 2010, p. 97). Although issues of national interest are the focus, the particular focus for this article is where national security is threatened through ICT. Furthermore, cyber attacks against individuals or individual firms are not of interest to this article. However, as will be illustrated in the "0x Omar"-Israeli case below, what at first may appear as isolated attacks against particular organisations, may in reality be the beginning of an orchestrated attack against key national infrastructure. In the latter case, such cyber attacks do fall within the scope of national security policies.

Definitions of national security tend to 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 two categories of determinants of power, natural and 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) concern the ways in which the people of a nation organise themselves and the manner in which they alter their environment (Jablonsky, 2002).

2.2. Cyberwar

The United Nations (UN) distinguishes between cyber crime and cyberwar. The politico-military stream deals with the notion of cyberwar, whereas the economic stream deals with cyber crime (Maurere, 2011). The focus for this article is on the politico-military, although as the "0x Omar"-Israeli conflict will illustrate, the distinctions drawn by the UN are inadequate, in that a cyber attack can begin guised as cyber crime.

The best known example of what cyberwar is today was an attack perpetrated against Estonia. Although the example is well publicised, what is difficult to prove is who the aggressor was. Shackelford (2009, p. 18) stated that: "Determining who was responsible for this cyber attack is the murkiest problem facing authorities in the aftermath of the Estonian assault." Similarly in the "0x Omar"-Israeli case below, analysis of the attacks initially led to views that they originated in Mexico, and later proved inconclusive. Thus in modern cyberdefence, determining who the aggressors are and against whom to take retaliatory action, can be a difficult matter. This influences the way policy development takes place, in terms of defensive strategies and counter-measures.

2.3. Policy as a risk mitigation strategy

The link between ethics and public policy is not new. People have addressed this link in relation to various policies, ranging from universal access to technology (Arch & Burmeister, 2003), to policies governing international use of ICT (Burmeister, 2013), and also to security policies (Boston, Bradstock, & Eng, 2010; Irwin, 2002; Loannides & Tondini, 2010). For instance, Boston, Bradstock and Eng (2010, p. 1) pointed out that "ethics is about what we ought to do or ought not do ... (and that) it is generally accepted that the domain of ethics embraces not merely the discrete actions of individuals but also the actions of groups ... such as nations." They argued that ethical inquiry is relevant to the public realm. This is not to suggest that cybersecurity policy should be solely concerned with ethics, but rather, that questions around what should be the response to a threat of national security (what ought to be done), are ethical concerns. The policy needs to cater to a broad spectrum, both the consequentialist focus of consequences of implementing the policy, and the non-consequentialist approaches of ensuring compliance with national values. Aside from dealing with conflicting ethical frameworks, policies are not created in political vacuums. Instead, they are developed in the midst of "converging/conflicting political agendas and approaches" (Loannides & Tondini, 2010, p. 8).

The co-ordinated cyber attacks in Estonia in 2007 against telecommunication companies, government agencies, banks and other critical information infrastructure sent shock waves around the world with regard to cyberspace vulnerabilities that resulted in direct threats to national security. Governments around the world have in

response, established policies that govern interaction and collaboration between Government entities, private sector, academia and civil society in collective efforts to mitigate cyber security vulnerabilities and attacks. One of the responsibilities of government is to put in place strategies that ensure that if attacked, the nation is able to defend its interests. For example, in discussing the effects of the phenomenon of globalisation on the pursuit of national security, Phahlamohlaka (2010, p. 101) claimed that "National military doctrines are abandoning offence in favour of defence or deterrence". Such strategies are implemented according to legislated policies, as exemplified by the Department of Defence who argued in favour of a national security policy, and called for "a national effort to ensure the security of increasingly vulnerable and interconnected infrastructures in the United States" (Shackelford, 2008, p 13).

A comprehensive review of cyber security policies was conducted in 2011, to inform the soon to be adopted cyber security policy of South Africa. Phahlamohlaka, van Vuuren and Coetzee (2011) reviewed the policies of the USA, Canada, South Korea, the UK, China, Georgia, and Iran, as well as the draft RSA policy, which in large part borrowed from the Finnish cyber security policy. Their review revealed that many nations have instituted policies to protect their sovereign interests from cyber attacks. For example, the USA:

> *… created a Cyber Command (CYBERCOM) under the Strategic Command led by the head of the National Security Agency (NSA), who reports directly to the President. The main reason stated was that the current capabilities to operate in cyberspace have outpaced the development of policy, law and precedent to guide and control these operations. (Phahlamohlaka et al., 2011, p. 1)*

They also distinguished policies in developed countries, from those in developing nations such as South Africa. Developing nations face the dilemma that in order to catch up with the rest of the world, their need to increase connectivity to the Internet also increases the cyber security risks that accompany the connectivity.

> *What has brought the US nation to a crossroads because of over-reliance on cyberspace is exactly what developing nations are aspiring for- ironical as it might sound. The bottom line here is that developing nations have no option, but to be part of the cyber citizenry. (Phahlamohlaka et al., 2011, p. 2)*

3. "0x Omar"-Israeli case

The context for discussing the South African policy is the 2012 exchange of cyber conflict between "0x Omar" and Israel. The method of investigation involved the following discourse analysis.

3.1. Data collection and data analysis

The keyword inserted in a Google search engine was "0x Omar" in Arabic; this was the nickname of the hacker who presumably lived in Saudi Arabia. The Google search, which took place during the month of April 2012, returned 54 pages worth of results. All of these results were examined. To make sure no story about these attacks was missed, another separate complementary search within the archives of local Saudi journalistic websites including Sabq.org and AlArabiya.net was also carried out. An additional search used the keyword "0x Omar" (in English) and was conducted at the same time the

previous search was performed. The data collected through the above searches were analyzed as they were collected. The focus of the analysis was on the occurrence of information relating to hacking attacks by the presumed hackers of these two nations. Specifically, the searches tried to address the following questions: who attacked what? When? How? Why? What was stolen or denied access to? What was the reaction in response to the attack? The results of these searches are described below.

3.2. Results: "0x Omar"-Israeli case

At the beginning of 2012 a war erupted on cyberspace between "0x Omar" and Israel (http://www.alarabiya.net/views/2012/01/21/189527.html) raising an interesting question: will cyber warfare replace conventional military conflicts? It all started on January 3 when a Saudi hacker named "0x Omar" boasted that he had revealed the credit card information of over 400,000 Israeli credit card holders (http://www.defence.pk/forums/world-affairs/152613-saudi-arabian-hackers-releases-400-000-israeli-cc-details.html). When Israeli banks tried to underestimate the gravity of the attack, "0x Omar" struck again on January 5 revealing the details of 11,000 credit card holders (http://sabq.org/Mhbfde). On January 6 an Israeli student claimed he revealed the identity of the hacker who according to him was a 19 year old man living in Mexico. The attacker, however, dismissed those claims challenging the whole world to find him.

In terms of the reaction to these attacks, a Saudi cyber security expert doubted that the hacker was a Saudi arguing that these were all journalistic stories and hypothesizing "may be cyber security companies are behind these attacks to market their products" (http://sabq.org/prbfde). A Saudi journalist, however, expressed serious concerns about the implications of these attacks, warning these could lead to cyber warfare between Israel and Saudi Arabia that could seriously threaten the Saudi electronic financial systems, and calling for Saudis not to applaud these hacking attacks so as not to intensify the situation (http://sabq.org/Onbfde). On the other hand, Hamas appeared very supportive of these attacks calling for more of these "means … to confront the Zionist crimes" and at least two Saudi scholars commented on the incident with the first praising the intention but criticizing the means (hacking) and the second hailing the attacks as an example of defeating the impossible (Israel) but while also criticizing the means to do that.

The Deputy Israeli Foreign Minister, Danny Ayalo, whose website was also hacked by "0x Omar" (http://www.youtube.ng/watch?v=SKzm6pEOGN0&feature=related), took the attacks very seriously saying these attacks were violations of Israeli sovereignty, equating the operation to a terrorist act, and warning those responsible that they would not go unpunished (http://sabq.org/gkbfde). In retaliation to the above hacking attacks, an Israeli youth revealed the details of hundreds of credit card holders from the Gulf and Iran keeping to himself only credit card CCV numbers (http://sabq.org/6ubfde). Several similar incidents of hacking and revelations of credit card information, email and Facebook accounts login information took place over the following days. Credit card users in both countries admitted being affected by the release of their credit information.
(http://www.alwatan.com.sa/Economy/News_Detail.aspx?ArticleID=82684&CategoryID=2; http://www.alquds.co.uk/index.asp?fname=today%5C11qpt946.htm&arc=data%5C2012%5C01%5C01-11%5C11qpt946.htm; http://sabq.org/Print/News/BRyno)

On January 16, 2012, two significant attacks occurred. Indeed, the hacking incidents took a different turn when "0x Omar" (the supposed Saudi hacker) and another took down the El Al (Israeli airline) and the Tel Aviv Stock Exchange websites (http://www.alyaum.com/News/art/40991.html). In retaliation, Israeli hackers first revealed the log-in information of 30,000 Facebook and email accounts; second, they revealed 10,000 additional email and Facebook accounts (http://sabq.org/Atbfde); third, they revealed the credit card information of 4,800 Saudi credit card holders; fourth, and most importantly, they brought down both the Saudi and the UAE stock exchange websites. In addition, Israeli hackers also shared an additional 25,000 Facebook and email accounts of Arab users.

In response, Saudi hackers launched a denial of service attack (of more than one million requests for access at the same time) on the biggest hospital in Israel (Sheba) bringing the site down for several hours (http://sabq.org/PLbfde). This led the Israeli hackers to hack into the Saudi Presidency of Metrology and Environment protection (http://sabq.org/1Mbfde) albeit the damage caused by this attack was not significant.

Perhaps the most important and significant attack of all these was hacking into the Israeli Air Force which resulted in the theft of huge amounts of sensitive information, including photo IDs and certificates. According to the media report, "0x Omar" made all these available for download from the internet (http://sabq.org/5qefde). It is not clear what happened after this. As of the writing of this article no more news were found in relation to these hacking incidents. It is quite possible that "0x Omar" was finally arrested as some Saudi online communities claimed.

4. "0x Omar"-Israeli implications for South African policy

South Africa has a population of over 51 million, with vast portions of the country in non-urban, rural parts of the country. To help its citizens to share in the information age, the national broadband infrastructure has been undergoing massive upgrades. The above cyber attack against Israel could have been launched against any nation. The Republic of South Africa (RSA) has developed a comprehensive policy framework (http://www.finpro.fi/documents/10304/70891291-c1bd-4c6b-8252-5040bb554d38; http://www.cyanre.co.za/national-cybersecurity-policy.pdf; http://www.justice.gov.za/m_speeches/2013/20130404-dm-cyberlaw.html; http://www.wolfpackrisk.com/south-africa-beefing-up-cyber-security/) to deal with sovereign threats to its national security, posed by cyber attacks. That development took place over the previous eight years and was approved by Cabinet of the RSA in March 2012, with a newer version expected to be released soon. In the next section, the historical need for and development of the RSA cybersecurity policy is briefly discussed, followed by a hypothetical discourse analysis of relevant elements of the South African cybersecurity policy framework in relation to ethical dimensions of the "0x Omar"-Israeli case. This is done in order to analyse the potential austerity and efficacy of the South African cybersecurity policy framework implementation within the context of national security.

4.1. Historical need for and development of the policy

As discussed above, the co-ordinated cyber attacks in Estonia resulted in governments around the world establishing policies to govern interaction and collaboration between Government entities, private sector, academia and civil society in collective efforts to

mitigate cyber security vulnerabilities and attacks. Although various initiatives existed, South Africa acknowledged that taken collectively, the then current initiatives did not adequately address the cyber security challenges that the country faced. Cyber attacks launched in recent years against advanced information societies aimed at undermining the functioning of public and private sector information systems. Such attacks placed the abuse of cyberspace high on the list of international and local security threats. South Africa took a stance that cyber threats needed to be addressed at both the global and national levels (Phahlamohlaka et al., 2011). The country considered these global cyber threats as serious and with high interests at stake. As a result, it proposed that comprehensive use of ICT solutions be supported by a high level of security measures and be embedded in a broad and sophisticated cyber security culture.

Like other countries, South Africa is increasingly becoming dependent on the Internet to conduct business and to provide social services to its people. A massive broadband rollout is currently under way which will bring connectivity to many citizens and their institutions. The unfortunate reality is that with increasing broadband access goes increasing vulnerability and thus increasing threats to national security. The RSA has an ethical obligation to ensure the safety of its public. For instance, despite its 10% internet penetration rate, South Africa is in the top three countries being targeted for phishing purposes, others being the USA and the UK (Van Vuuren, Phahlamohlaka, & Brazzoli, 2010). Similar to the United Kingdom's cyber strategy released in late 2011, RSA policy focuses on defence. This bellicose stance applies to both the military and private sectors (Grauman, 2012).

4.2. Ethical lessons arising from RSA policy

From an ethical viewpoint, the South African National Cybersecurity Policy Framework (NCPF) (Bapela, 2011; Nel, 2013) addresses what the response of the national services ought to be to preserve national values, including those of safety and security for its citizens. The NCPF is intended to provide a holistic approach pertaining to the promotion of cyber security measures by all role players (State, public, private sector, civil society and special interest groups) in relation to cyber security threats. It is necessitated to ensure a focused and all-embracing safety and security response in respect of the cyber security environment.

Rather than list the extensive policy in its entirety, key elements of it have been combined in Table 1, to bring together the ethical elements of the policy that are addressed by the "0x Omar"-Israeli case. Just as the full policy is not presented, neither are all ethical theories. For instance, Vallor (2013) has demonstrated that virtue ethics applies in military settings. That is, whilst war itself is not virtuous, certain military actions should be distinguished from criminal activities, just as in the context of this article, cyber crime should be distinguished from cyberwar. Vallor pointed out that virtues such as duty, honour and service are important ethical considerations for military personnel. However, in this article the focus is on nation-states, not individuals, and as such, virtue ethics are not considered in the policy discussion presented in Table 1.

Table 1: RSA policy elements considered in the light of the "0x Omar"-Israeli case

Ethical	**RSA policy**	**Lessons from "0x Omar"-Israeli**

considerations		case
What ought to be done or not done, from a big picture standpoint. Utilitarian perspectives encourage the consideration of the consequences, such as prematurely retaliating, when the identities of attackers is not certain.	The development and implementation of a Government led, coherent and integrated cyber security approach to address cyber security threats. Establishing a dedicated policy, strategy and decision making body to be known as the Justice Crime Prevention and Security (JCPS) Cybersecurity Response Committee, to identify and prioritise areas of intervention regarding cyber security related threats. The Cybersecurity Response Committee is chaired by the State Security Agency (SSA) and supported operationally by a Cybersecurity Centre, situated at the SSA. Coordination of the promotion of cyber security measures by all role players (State, public, private sector, civil society and special interest groups) in relation to cyber security threats, through interaction with and in conjunction with the Cybersecurity Hub, established within the Department of Communications.	The RSA policy statements reflect a focus on response mechanisms rather than offence. The "0x Omar"-Israeli case is a good example of why that is ethically appropriate, namely in relation to the notion of attribution. When attacked, the RSA would naturally want to retaliate and that requires the ability to determine the parties responsible for the attack. As seen in the "0x Omar"-Israeli situation, attribution when under cyber attack can be difficult. Where attribution is possible, it assists in avoiding punishing the innocent, and it links the attacking action to the retaliatory reaction in the minds of the attackers, RSA and global citizens. Initially the identity of the attacker was thought to be a 19 year old man living in Mexico, later it was presumed that the attack originated from Saudi Arabia. Even if so, was it the work of an isolated individual, or the work of a terrorist group, or an attack by another nation state? As pointed out by Applegate and Stavrou (2013), cyber conflict, rather than cyberwar may be involved, that is, rather than one nation state attacking another, it could be an attack by non-state actors, whose actions are politically motivated. Rapid response to defend South Africa, rather than rapid response to retaliate is thus an appropriate focus of the RSA policy.
Ethical decision making about whether an activity is cyber crime or cyberwar. Denotologically the state and	The capability to effectively coordinate departmental resources in the achievement of common cyber security safety and security objectives (including the planning,	0x Omar's attacks exposing credit card information and later denial of service attacks could have been instances of crime, not terrorism or warfare. It began with his revealing the information of 400,000 Israeli credit card holders. Yet the

private sectors have a duty or responsibility to protect their clients, customers and citizens.	response, coordination and monitoring, and evaluation). Measures to address national security threats in terms of cyberspace. Measures to build confidence and trust in the secure use of ICT. The development, review and updating of existing substantive and procedural laws to ensure alignment.	coordinated and sustained effort suggested that warfare was involved. Rapid and effective response requires close monitoring of cyber crime.
Government policy encourages ethical responses from the private sector. Ethical considerations need to be reflected not only in policy statements, but also in legal frameworks.	Strengthening of the intelligence collection, investigation, prosecution and judicial processes, in respect of preventing and addressing cybercrime, cyber terrorism and cyber warfare. Ensuring the protection of national critical information infrastructure. The promotion of a cyber security culture and compliance with minimum security standards. The establishment of public-private partnership action plans in line with the NCPF. Ensuring a comprehensive legal framework governing cyberspace.	The "0x Omar"-Israeli case demonstrates that private citizens in both countries escalated the events, taking vigilante actions, yet in retaliating against presumed attackers, widened the conflict. For instance, Israeli hackers cast a wide net, retaliating not only against Saudi Arabia, but other sovereign nation states in the middle east. The RSA policy also addresses the need to inform the public, to promote trust and confidence in state responses, and to ensure that appropriate legal measures exist to support their actions in response to cyberwar threats. Together these aid in the mitigation of those threats.

Absent from Table 1 is an answer to a question such as, at what point does the policy require a nation state to prepare for a cyber offence in response to a cyber attack? The RSA only addresses defence and not offence. Its focus is on response mechanisms rather than offence. In this regard, South Africa subjects itself to international instruments under the auspices of the United Nations, as cybersecurity is by its nature a global problem that requires international, regional and national solutions.

5. Conclusion

Since ancient times one nation has attacked another. Policies to address threats to national security exist to ensure that the risks posed by such threats can be countered. Although policies go beyond ethical considerations, in the main the actions such policies advocate reflect an ethical response to the threats posed. Ethical considerations help in judging duties and consequences, thus aiding in the determination of mitigating factors.

Boston et al. (2010) described policy in ethical terms, even though philosophers debate whether group morality, including collective responsibility is even possible, as opposed to individual moral agency (Smiley, 2010). But in the light of cyber attacks, a collective response to real threats against sensitive infrastructure and individual citizens is required. As nations increase the provision of high speed internet access for the wider society, so threats of cyber attacks increase. The opportunity provided by the technology is thus implicitly accompanied by its own threats. ICT is blurring the lines, and affecting the debate about individual responsibility versus collective responsibility. Aggression against a nation state requires the collective, not the individual to respond.

The RSA has taken ethical steps within a particular political milieu, to create a national cyber security policy which addresses the very real threat that new infrastructure invites from cyber criminals, including threats to the nation as a whole. As seen in the discussion above, attribution is often difficult because the attacks can be perpetrated not only by combatant states, but also by non-state actors, individuals or criminal organisations. This is one reason why the RSA only addresses defence and not offence. Defending against such attacks effectively requires careful planning and preparation, so that national interests can be safe-guarded in timely and effective ways. All governments, not just South Africa, need to face this challenge.

References

Applegate, S. D., & Stavrou, A. (2013). *Towards a Cyber Conflict Taxonomy.* Paper presented at the 5th International Conference on Cyber Conflict, Tallinn.

Arch, A., & Burmeister, O. K. (2003). Australian Policy Experiences post Sydney Olympic Games. *Information Technology and Disabilities, 9*(2).

Bapela, O. (2011). Cybersecurity Policy and Legal Framework From a South African Perspective *Summit on Information and Network Security for Emerging Markets*.

Boston, J., Bradstock, A., & Eng, D. L. (2010). Ethics and public policy. In J. Boston, A. Bradstock & D. L. Eng (Eds.), *Public policy: why ethics matters* (pp. 1-17). Canberra: ANU E Press.

Burmeister, O. K. (2013). Achieving the goal of a global computing code of ethics through an international-localisation hybrid. *Ethical Space: The International Journal of Communication Ethics, 10*(4), 25-32.

Grauman, B. (2012). *Cyber-security: The vexed question of global rules*. Brussels: Security & Defence Agenda.

Irwin, R. (2002). Linking Ethics and Security in Canadian Foreign Policy. In R. Irwin (Ed.), *Ethics and Security in Canadian Foreign Policy* (pp. 3-13). Toronto, Ontario: UTP Distribution.

Jablonsky, D. (2002). *The State of the National Security State*. Carlisle, PA: US Army War College.

Loannides, I., & Tondini, M. (2010). D.3.5. Policy recommendation report on implications of the changing relation between the ethical dilemmas of internal/external security (pp. 182). Amsterdam: Department of Governance Studies, VU University Amsterdam.

Maurere, T. (2011). *Cyber Norm Emergence at the United Nations: An Analysis of the UN's Activities Regarding Cyber Security*. Cambridge, MA: Belfer Center for Science and International Affairs, Harvard Kennedy School.

Nel, A. (2013). *Advancement of Cyberlaw and Information Ethics in Africa and Globally*. Pretoria, South Africa: Lex Informatika.

Phahlamohlaka, L. J. (2010). *Globalisation and national security issues for the state: implications for national ICT policies* (Vol. 282). Boston: Springer.

Phahlamohlaka, L. J., Modise, M., & Nengovhela, N. (2008). *Digital divide: a national security argumentative analysis within a South African context.* Paper presented at the IFIP TC9 ICT uses in Warfare and the Safeguarding of Peace, Pretoria, South Africa.

Phahlamohlaka, L. J., van Vuuren, J. C. J., & Coetzee, A. J. (2011). *Cyber Security Awareness Toolkit for National Security: an Approach to South Africa's Cyber Security Policy Implementation.* Paper presented at the First IFIP TC9 / TC11 Southern African Cyber Security Awareness Workshop Gaborone, Botswana.

Shackelford, S. J. (2009). From Nuclear War to Net War: Analogizing Cyber Attacks in International Law. *Berkley Journal of International Law, 25*(3), 191-250.

Smiley, M. (2010). Collective Responsibility. In E. N. Zalta (Ed.), *The Stanford Encyclopedia of Philosophy* (Winter 2012 Edition ed.).

Vallor, S. (2013). *The Future of Military Virtue: Autonomous Systems and the Moral Deskilling of the Military.* Paper presented at the 5th International Conference on Cyber Conflict, Tallinn.

Van Vuuren, J. C. J., Phahlamohlaka, L. J., & Brazzoli, M. (2010). *The Impact of the Increase in Broadband Access on South African National Security and the Average Citizen.* Paper presented at the Workshop on ICT Uses in Warfare and the Safeguarding of Peace, Bela Bela, South Africa.