Proposed Model for a Cybersecurity Centre of Innovation for South Africa

Joey Jansen van Vuuren, Marthie Grobler, Louise Leenen, and Jackie Phahlamohlaka

DPSS, CSIR, Pretoria, South Africa
{jjvvuuren, mgrobler1, lleenen, jphahlamohlaka}@csir.co.za

Abstract Most communications in the new era are dependent on Information and Communication Technology (ICT). In addition, infrastructure is becoming increasingly interconnected. This not only makes lives easier, but also leaves technology users more vulnerable. Cybercrime, digital espionage and other cyber disturbances dictate the news reports on a daily basis. In general, cyber-attacks are no longer confined to small-scale rogue hackers. Cyber-attacks are now a part of organised crime and the underground economy, posing a real threat to critical infrastructure; possibly with state actors driving these actions. The responsibility to protect ICT stretches beyond individual companies, sectors and even beyond nations. The authors of this paper propose a Cybersecurity Centre Of Innovation (CCOI) as a central point for the South African government, business and academia to create a secure cyber space for the country: a cyber space without crime that is resilient and resistant to disruptions; a cyber space that promotes innovation, helps the economy and enhances national security. The key driver of the proposed CCOI is collaboration; solutions to cyber risks require a combined approach. This paper describes the organisational structure, functions, activities and benefits of a CCOI.

Keywords: Cybersecurity, South Africa, Centre of Innovation, national security

1 Introduction

The increase in African broadband access has had a significant impact on Internet access in South Africa. More rural communities are becoming integrated into the global village due to increased hardware and software corporate donations, the proliferation of mobile Internet devices and government programmes aimed at bridging the digital divide through major broadband expansion projects. These measures facilitate the rapid growth in the number of South African Internet citizens through desktop or laptop computers, iPads and mobile phones. South Africa currently has a greater exposure to cyber threats than before the significant increase in broadband availability in 2009 (Jansen van Vuuren et al. 2010); however, a large percentage of the population have not received adequate training in cybersecurity awareness, nor regular and sustained exposure to technological devices and broadband Internet access. An additional threat is that South Africa in many ways serves as the Internet entry point to the

© Springer-Verlag Berlin Heidelberg 2011

African continent and could therefore be used as a central point for launching cyber warfare type attacks on the rest of the world. Cybersecurity has therefore been identified as a critical component contributing towards National Security in South Africa. (Jansen van Vuuren et al. 2009)

A particularly serious dimension of the cyber domain is that attacks and crimes may be orchestrated from anywhere in the world. Many countries do not have effective laws to deal with cyber crime, and there are not sufficient international collaboration and standards in place yet to deal with the complexity of these crimes and attacks.

The next section provides a motivation for the establishment of a South African Cybersecurity Centre of Innovation.

2 Motivation

South Africa has largely kept up with the global ICT trends and usage. While overall Internet penetration is still fairly low, in most provinces less than 10% (StatsSA 2012), the use of Internet today is essential for government, business and organisations. Further ICT development in South Africa, such as increased penetration of broad bandwidth Internet access, will lead to an exponential increase in risks as inadequate user experience, awareness and sophistication lead to increased vulnerability to cyber threats, even when counter measures exist (this holds at individual, organisation and government level).

While South Africa has not had a major cyber-attack similar to recent attacks on the United States, Estonia, Korea, the United Kingdom, Iran and Georgia, evidence points to the real possibility of an attack. Information from the South African Police Service and other sources indicate the existence of botnets (controllable malware clandestinely installed on a computer), as well as botnet control servers on South African networks. In general, these risks and threats cause a lack of confidentiality, integrity and availability of information and ICT systems belonging to government, business and citizens. Although technology is not the only defence, when threats spread within seconds they can no longer be dealt with through human intervention - technology is required to implement resilient network and service infrastructures that can mitigate against such threats. The nature of ICT systems makes it possible for a single incident to affect all systems that are connected in the same network. It is therefore not sufficient for an individual firm or government to work in solo on resolving these incidents.

Currently, the majority of Internet users in South Africa have access to the Internet from their workplaces or via their mobile phones (Jansen van Vuuren et al. 2012). These developments indicate that South Africans are becoming more active online. In addition, an online environment has no border control such as employed in physical borders. There is no police force to guard against those entering the country online. This means that everyone who goes online is on his/her own regarding malicious and criminal activities. Users cannot protect themselves adequately from these incidents. The current situation in South Africa is that each role player in the ICT industry has their own response mechanism, of which most are not congruent with their clients,

neighbours and competitors. While there is significant cyber security expertise in South Africa, the country is at risk because there is neither a national understanding nor a coherent action plan in terms of addressing cybercrime in South Africa.

In this paper the authors argue that the establishment of a Cybersecurity Centre of Innovation (CCOI) should rectify this situation. The aim of CCOI is to offer a platform for collaboration of all entities that can contribute to a secure cyberspace for South Africa.

Section 3 gives an overview of similar initiatives on other countries. In Section 4 the authors give an outline of the structure, function activities, opportunities and benefits of a CCOI. The paper is concluded in Section 5.

3 Similar Initiatives

A number of international cyber security innovation initiatives have been launched. This section provides an overview of some of these initiatives which serve as input to the Cybersecurity Centre of Innovation.

3.1 Advanced Cyber Security Center (ACSC)

ASCS is a not-for-profit consortium that was launched and supported by Mass Insight Global Partnerships. From its offices at MITRE in Bedford, Massachusetts, the Advanced Cyber Security Center uses the advantage of New England's unparalleled academic, industrial and research resources to develop next-generation solutions and strategies for protecting the nation's public and private IT infrastructure. The centre focuses on sharing cyber threat information, the development of innovative ways to address the most advanced cyber threats in next-generation cybersecurity research and development, as well as creating education programmes that will address the shortfall in cyber talent (ASCS 2013). The centre also functions as a cybersecurity operations centre (MITRE Corporation n.d.).

The centre has three key initiatives:

- Information sharing between expert practitioners and researchers to conduct threat analysis; identification of new threat indicators and the sharing of best practices under a Non-Disclosure Agreement. A cyber portal is used to share sensitive real-time threat information, building on the trust established at the "in person" sessions.
- Research and development, and education where cybersecurity solutions are developed to address cybersecurity gaps. Provision of graduate education opportunities for new talent in the cybersecurity field.
- Development of policies for federal legislation and the establishment of ASCS as best practice laboratory.

3.2 NexGen Cyber Innovation and Technology Center

The NexGen Cyber Innovation and Technology Center is aimed at preserving and protecting Lockheed Martin customer missions and addresses the greater cybersecurity challenges worldwide. It is a world-class centre designed for cyber research and development, customer and partner collaboration and innovation. At the centre, Lockheed Martin and partner technologies are integrated to create rapid prototypes to speed the innovation of solution delivery and provide seamless security. Through this meshing of innovation, technology and talent, Lockheed Martin and its partners work to solve the most difficult cyber challenges and help customers to define their own solutions (Lockheed Martin 2013).

The centre is fully equipped for live cyber technology exercises and demonstrations to help customers integrate solutions and test them in environments that are representative of their missions. The centre is the anchor point for a new Global Cyber Innovation range, enabling safe testing in both simulated and real world environments for the development of integrated cyber solutions. Some of the centre's key features include:

- Seven collaboration areas.
- A Global Cyber range.
- Cloud computing platforms.
- A green IT data center (Lockheed Martin 2013).

3.3 Cyber Innovation Centre (CIC)

The CIC is a not-for-profit corporation located in Bossier City, Louisiana that has been established to meet growing cyber demands by promoting research, education, and technological innovation and transfer of knowledge with strategic alliances between governmental agencies, private industry and academic institutions. In order to achieve this they partner with the United States government (National Security Agency and Department of Homeland Security), industry, research and academia. The CIC uses their National Integrated Cyber Education Research Center (NICERC) to create a knowledge-based workforce and to do academic outreach.

The CIC goals are to:

- Stimulate innovation-based economic growth through strategic partnerships.
- Develop a knowledge-based workforce.
- Foster collaboration and serve as a conduit for governmental agencies, private industries and academic institutions to share ideas and advance research.
- Build the necessary critical infrastructure that will attract federal programs to the area (Cyber Innovation Centre 2013).

3.4 Centre for Cyber Security Sciences (CCySS)

The CCySS in the United Kingdom was created in early 2011. It is based on the work done by research groups within the City University of London's School of Engineering and Mathematical Sciences, the School of Informatics and the Cass Business

School (City University London n.d.). The Centre is invaluable through its combination of expertise in reliability, safety and security in audit and risk management. CCySS focuses its work in three critical areas. These are:

- Impact of cybersecurity on business, including impact on information risk governance, economics of security, information risk decisions.
- Security of the Internet, World Wide Web and cloud, and a deep analysis of related attacks.
- The evaluation and communication of the dependability and trustworthiness of complex socio-technical systems, using formal, rigorous and quantitative methods and associated evidence.

The centre's organisational structure is made up of nine core members and eight associate members. These members are active in contributing to the university's undergraduate and postgraduate programmes. The centre supports the doctoral students in research areas related to cybersecurity (City University London n.d.).

3.5 Academic Centre of Excellence for Cyber Security Research

The Academic Centre of Excellence for Cyber Security Research in the United Kingdom was created in 2012. The Centre is home to leading researchers, covering a wide range of cybersecurity related areas, including cryptography, human factors in security, end-to-end systems security, language-based security, program verification and analysis, automated program analysis, verification of computer software, vulnerability discovery, malware analysis and classification of code and the improved defences and mitigations (EPSRC (Engineering and Physical Sciences Research Council) 2013).

The Centre is tasked to assist the United Kingdom government, businesses and consumers in being more resilient to cyber-attacks by extending knowledge and enhancing skills in cybersecurity. In particular, the centre is tasked to:

- Enhance the United Kingdom's cyber knowledge base, skills and capability through original research.
- Provide top quality graduates in the field of cyber security.
- Support GCHQ's (the parent company) cybersecurity mission.
- Drive up the advancements and the level of innovation (Information Security Group, 2013).
- Address cybercrime and make the United Kingdom one of the most secure places in the world to do business in cyber space.
- Help to shape an open, vibrant and stable cyberspace which the United Kingdom public can use safely and that supports open societies (EPSRC (Engineering and Physical Sciences Research Council) 2012).

This research will allow leading United Kingdom academics in the field of cybersecurity to connect with industry security experts and international researchers to tackle some of the United Kingdom's toughest challenges in cybersecurity. This collaborative approach between academia, industry and government will ensure that research is

relevant and inspired by real world, cutting edge, security issues (EPSRC (Engineering and Physical Sciences Research Council) 2013).

3.6 Research Institute in the Science of Cyber Security (RISCC)

RISCC was created in 2012 at the University College London in the United Kingdom. The institute will work alongside the University of Aberdeen, Imperial College, Queen Mary College, Royal Holloway, Newcastle University and Northumbria University (Kaelin 2012).

The institute is focused on giving organisations more evidence to allow them to make better decisions, aiding in the development of cybersecurity as a science. It collects evidence about what degree of risk mitigation can be achieved through a particular method, including the costs of its introduction and on-going costs such as the impact on productivity, to balance the total cost of ownership against the risk. The institute's main goal is to move security from common, established practice to an evidence base, the same way it happened in medicine (UCL 2013). The institute will focus on four research areas:

- Productive security by assistance to decision makers in the field of information security to make more optimal choices with respect to both the security and productivity of organisations.
- Choice architecture for information security by the establishment of rigorous mathematical approaches to include uncertainty about unknowns in cybersecurity analysis in an attempt to derive a theory about the value of rigour. Research is done in terms of consumerisation, or the use in the workplace of people's own technologies.
- Games and abstraction to make better decisions and the development of new approaches to decision support based on game theory.
- Cybersecurity cartographies explore the methods that security managers use to develop, maintain and the use of visibility of both social and technical asset compliance behaviours for the management of cybersecurity risks (UCL 2013).

3.7 Global Cyber Security Capacity Building Centre (GCSCBC)

The aim of the GCSCBC (also referred to as the United Kingdom Cybersecurity Hub) is to understand how to deliver effective cyber security both within the United Kingdom and internationally. Its aim is to make this knowledge available to governments, communities and organisations to underpin the increase of their capacity in ways appropriate to ensuring a cyberspace which can continue to grow and innovate in support of well-being, human rights and prosperity for all (University of Oxford n.d.-a)

The GCSCBC is focused on developing a framework for understanding what works and what does not work across all cybersecurity dimensions in order to identify and adopt policies which have the potential to significantly enhance our safety and securi-

ty in cyberspace in ways that respect other core values and interests, such as in privacy and freedom of expression (University of Oxford n.d.-a).

The GCSCBC is focused on helping the international community increase the impact, scale and pace of cyber security capacity building by:

- Investigating the drivers for current capacity building activities and the conditions required to increase resources.
- Providing the scientific framework to enable individuals and institutions to measure and understand effective cybersecurity, providing an evidence base and model for supporting benchmarking, policy formation and measuring effectiveness.
- Pooling, evaluating and sharing information on best practice and experiences in capacity building activities.
- Creating and keeping up to date a critical guide to global expertise on cybersecurity.
- Setting out what needs to be done in order to analyse priorities, and identify and close gaps in the global response (University of Oxford n.d.-b).

3.8 The Hague Security Delta (HSD) Cybersecurity

The HSD Cybersecurity in the Netherlands is a security cluster where companies, governments and research institutions work together on innovations and knowledge in the field of cybersecurity, national and urban security, protection of critical infrastructure and forensics. It was initiated by a consortium of Netherlands Organisation for Applied Scientific Research (TNO), Twynstra Gudde, the Hague University of Applied Sciences, HCSS, the Chamber of Commerce, the Netherlands Forensic Institute and the West Holland Foreign Investment Agency (HSD, 2013). The most important initiatives include:

- The Cyber Security Academy's main initiatives are a master's program in Cybersecurity and a cybersecurity traineeship that is done in close cooperation with both public and private partners. Their facilities also include a communal place or 'campus', where professionals, researchers and students meet for education, research and sharing expertise in the field of cybersecurity.
- The Cyber Incident Experience Lab is used as a gaming lab where professionals and (top) managers gain new experience, insights and knowledge with respect to cybersecurity in familiar, challenging and real environments.

4 Cybersecurity Centre of Innovation for South Africa

This section contains details on the functions, constituency, organisational structure and benefits of the proposed centre.

The authors' preferred model amongst the similar initiatives is the ACSC discussed in Section 3.1. ACSC has managed to establish efficient processes to share information

amongst government agencies, industries and academic institutions, and they have strong academic support. ACSC is funded by government and industry.

4.1 Functions

A key aspect of the centre is collaboration, since no single organisation can respond effectively taking into account that:

- Attacks are increasing in sophistication.
- Current solutions are not adequate.
- Organisations want to increase the training and and sophistication of their employees and solutions (Jansen van Vuuren 2014).

The CCOI should aim to establish a partnership between businesses and industry, academia, government and research institutions and to provide these partners with a greater understanding of cybercrime and practical applications in terms of defending against these crimes. The diagram below describes the benefits of such collaboration.

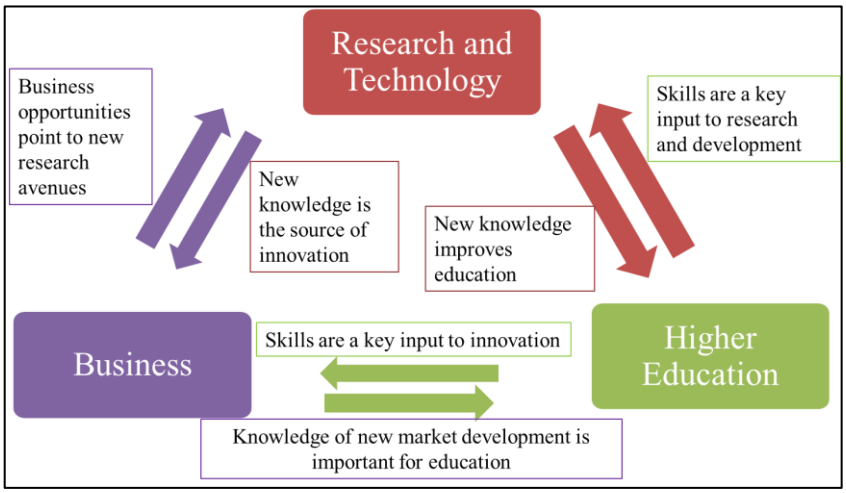

Fig. 1. Benefits of Business, Academia and Research Collaboration

This CCOI must be the central point of collaboration for cybersecurity activities in South Africa. It must serve the South African cyber community by focusing on:

- Cybersecurity related information sharing.
- Cybersecurity education and awareness.
- Cybersecurity research, development and innovation.

In addition, the CCOI must aim to be a world-class institution designed for cyber research and development, customer and partner collaboration and innovation, fully equipped for live cyber technology exercises and demonstrations required by industry and must be able to do safe testing in both simulated and real world environments for development of integrated cyber solutions.

Three key activities of the CCOI are discussed below.

The first key activity, cybersecurity information sharing, will be the coordination of collaboration to bring together expert practitioners and researchers in the field of cybersecurity.

This includes:

- Building cross sector networks and personal relations.
- Sharing best practices under a Non-Disclosure Agreement.
- Arrange technical exchange meetings for the exchange of technical information building of personal relationships among front-line cyber operations experts.
- Identify new threat indicators.
- Set-up and maintenance of a secure Cybersecurity Web Portal to enhance information sharing and access to key data.
- Collaboration with the South African Cybersecurity Hub (National Cyber Security Incident Response Team), the centre to be established by the Department of Communication with the objective to pool public and private sector threat information for the purposes of processing and disseminating such information to relevant stakeholders and to promote cybersecurity in South Africa.

The second key activity, cybersecurity education and awareness, will be to expand education opportunities for workforce and pipeline in the cyber security field.

This includes:

- Development of new cybersecurity qualifications and certifications.
- Expansion of education opportunities for pipeline and knowledge workers in the cybersecurity field.
- Availability of bursaries, internships and studentships.
- Hosting live cyber technology exercises and demonstrations required by industry.
- Cybersecurity awareness training for industry and citizen to gain an improvement of cybersecurity awareness for the workforce and citizens.

The third key activity, cybersecurity research, development and innovation, will be research with the focus to development innovation solutions to improve cybersecurity.

This includes:

- Cybersecurity research to improve cybersecurity and address cybersecurity gaps.
- Development of innovative cybersecurity solutions and patents.
- Appointing qualified research chairs.
- Conducting quantitative cybersecurity threat analysis and red teaming.
- Perform safe testing in both a simulated and real world environment for development of integrated cybersecurity solutions.

- Development of a scientific framework to enable individuals and institutions to measure and understand effective cybersecurity.
- Provide support for policy development and legislation.
- Protection and resilience of society, focusing on the government as a policy maker and regulator.

Cybersecurity research and development will mostly be funded by government and National Research Foundation where intellectual property (IP) will be open. Research support for industry will result in the propriety of IP.

4.2 Organisational Structure

The envisioned management and staffing requirements for the Cybersecurity Centre of Innovation is presented in **Fig. 2**.

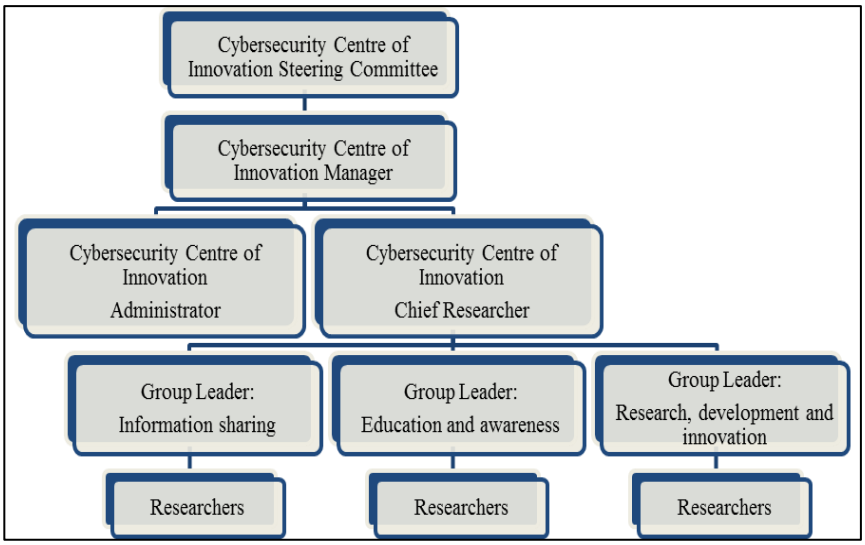

Fig. 2. Proposed Cybersecurity Centre of Innovation Management and Staffing

4.3 Constituency

Fig. 3 shows the relationships between the constituency partners of the CCOI. The CCOI will serve as a central point for the South African businesses and industry, the academia and higher education institutions, local and international research institutions and the South African government in terms of cybersecurity. In addition, the CCIO will have a direct relationship with the South African Cybersecurity Hub.

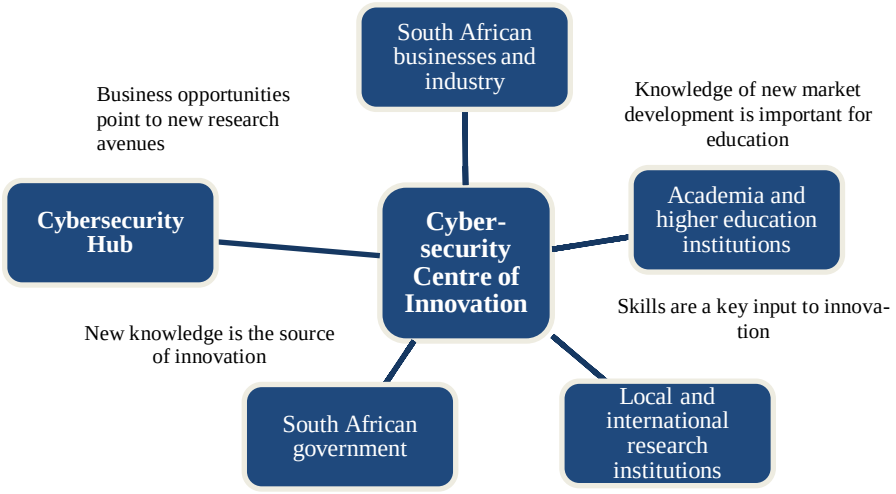

Fig. 3. Proposed Cybersecurity Centre of Innovation Relationships

The role-players that have been identified include, but are not limited to, the following:

- South African businesses and industry consisting mainly of South African Banking Risk Information Centre (SABRIC), Security Operations Centres and Internet Service Providers.
- Academia and higher education institutions.
- Local and international research institutions.
- South African government departments.
- International Collaboration
    - The International Multilateral Partnership Against Cyber Threats (IMPACT) is the cybersecurity executing arm of the United Nations' specialised agency - (ITU). As the world's first UN-backed comprehensive alliance against cyber threats, IMPACT brings together governments, academia and industry experts to enhance the global community's capabilities in dealing with cyber threats.
    - International Centres of Cybersecurity Innovation.

4.4 Opportunities and benefits

Some of the opportunities that the CCOI can pursue are:

- Collaborative development of technological competencies, as well as research, development and innovation leading to commercialisation or transfer of research, development and innovation industrialisation in the cybersecurity field.
- Establishing a recognisable hub for coordinated cybersecurity research, development and innovation.

- Contributing to building a new generation of cybersecurity specialists.
- Linking and strengthening cybersecurity pockets of excellence, both locally and internationally.
- Entrepreneurial activity through research-industry partnerships and the transfer of research results to the CCOI partners.
- Developing mechanisms for stakeholders to articulate needs and influence research and human capital development agendas.
- Enabling the community to utilise the implementation of South African ICT legislation and related standardisation.

Some of the identified benefits of establishing a CCOI include:

- National recognition regarding collaboration with the South African Cybersecurity Hub.
- Enabling cybersecurity-related early warning systems.
- A less vulnerable South Africa due to an increased and thorough understanding and operational response to cybersecurity threats.
- Protecting critical infrastructures based on a national information security strategy as well as local and international collaboration.
- Utilising the local ICT industry and expertise in a joint effort towards the investigation and combating of cybercrimes.
- Enabling the flow of innovation and knowledge from research to industrial and economic activities.
- Collaborating efforts in terms of cybersecurity research, development and innovation should result in a less fragmented national cybersecurity effort, with fewer overlaps and duplications of research, development and innovation efforts.

4.5 Key challenges

The proposed centre has to address challenges that are specific to South Africa:

- Only the banking sector has managed to establish collaboration in terms of cybersecurity information exchange. Government and the rest of the private sector will have to establish similar collaborations.
- Academic institutions offer no formal qualifications in cybersecurity and no such curricula exist yet. This challenge can be addressed by establishing a group responsible for the curriculation of formal cybersecurity qualifications.

5 Conclusion

The establishment of the CCOI in South Africa is essential to combat the current cybersecurity threat. However, processes in South Africa make it difficult to establish collaboration. For example, although the establishment of the South African Cybersecurity Hub has started already in 2011, it is not yet operational and therefore the inherent value of collaborating with this entity cannot be fully understood. In addition,

the National Cybersecurity Policy Framework and policies have not been published yet. As a result, many of the South African stakeholders are not comfortable to engage in any concrete action in terms of cybersecurity and cybersecurity collaboration. One of the reasons for the difficulty in establishing collaboration may be the lack of skills in cybersecurity. Another reason is that cybersecurity a rather vague and undefined concept. As such, there exist no concrete international agreement on the definition of cybersecurity or what exactly it is comprised of. In addition, the cyber domain tends to be volatile and fast changing, creating a competitive environment in which role players tend not to share information. This is partly because the domain is not clearly understood and roleplayers do not want to share their own personal information, but also because they do not want to give competitors an advantage in terms of work already done. Other countries experienced similar difficulties and this resulted in the development of cybersecurity innovation centres elsewhere.

An urgent need for international agreement on the definition of cybersecurity, as well as the definition of cybersecurity standards. Some efforts have been made by ISO/IEC 27032, but this standard is not commonly adopted by countries.

References

1. ASCS (2013) Advanced Cyber Security Centre http://www.acscenter.org/ Accessed 6 November 2013
2. City University London (n.d.) Centre for Cyber Security Sciences (CCySS). http://www.city.ac.uk/engineering-maths/research/cross-discipline-centres-and-groups/centre-for-cyber-security-sciences Accessed October, 30 2013
3. Cyber Innovation Centre (2013) Welcome TO CYBER INNOVATION CENTER. Accessed October 31 2013
4. EPSRC (Engineering and Physical Sciences Research Council) (2012) UK's first academic research institute to investigate the "science of cyber security". http://www.epsrc.ac.uk/newsevents/ news/2012/Pages/scienceofcybersecurity.aspx. Accessed 6 November 2013
5. EPSRC (Engineering and Physical Sciences Research Council) (2013) UK's second cyber research institute launched. http://www.epsrc.ac.uk/newsevents/news/2013/Pages/secondcyber researchinstitute.aspx. Accessed 6 November 2013
6. Jansen van Vuuren J, Grobler M, Zaaiman J (2012) Cyber Security Awareness as Critical Driver to National Security. International Journal of Cyber Warfare and Terrorism (IJCWT) 2 (1):27-38
7. Jansen van Vuuren J, Phahlamohlaka J, Brazzoli M (2009) The impact of the increase in broadband access on South African national security and the average citizen. Paper presented at the Information Warfare and Security, Airforce Institute of Technology, April 2010
8. Jansen van Vuuren J, Phahlamohlaka J, Brazzoli M (2010) The Impact of the Increase in Broadband Access on National Security and the Average citizen. Journal of Information Warfare 5:171-181
9. Jansen van Vuuren JC (2014) Cybersecurity Centre of Innovation. Cyber Shield, 5 edn. Wolf Pack, Johannesburg, South Africa

10. Kaelin (2012) UK's GCHQ announces a new cyber security institute. Available from: (Accessed 6 November 2013). http://www.techspot.com/news/50154-uks-gchq-announces-a-new-cyber-security-institute.html. Accessed 30 October 2013
11. Lockheed Martin (2013) NexGen Cyber Innovation & Technology Center http://www.lockheedmartin.com/us/isgs/nexgen.html. Accessed October 30 2013
12. MITRE Corporation (n.d.) The Advanced Cyber Security Center (ACSC): A Cyber Threat Information Sharing Consortium https://www.ncsc.nl/binaries/en/conference/conference-2011/speakers/bruce-bakis/1/Bruce%252. Accessed October, 31 2013
13. StatsSA (2012) General household survey 2011 . vol PO318, https://www.statssa.gov.za/publications/P0318/P0318April2012.pdf. Accessed 10 April 2013.
14. UCL (2013) Research Institute In Science of Cybersecurity. http://www.ucl.ac.uk/ cyber-security/about_us. Accessed 30 October 2013
15. University of Oxford (n.d.-a) Cyber Security – The Global Cyber Security Capacity Centre. http://www.oxfordmartin.ox.ac.uk/institutes/cybersecurity Accessed 6 November 2013
16. University of Oxford (n.d.-b) Global Cyber Security Capacity Centre. http://www.oxfordmartin.ox.ac.uk/downloads/cybersecurity/Global%20Cyber%20Security%20Capacity%20Centre.pdf Accessed 6 November 2013