

https://dspace.org/

Guest Editor's Introduction: AJIC Focus Section on Cybersecurity

Pillay, Kiru

2017-12-23

http://hdl.handle.net/10539/23575

Pillay, K. (2017). Guest editor's introduction: AJIC focus section on cybersecurity. The African Journal of Information and Communication (AJIC), 20, 79-82. https://doi.org/10.23962/10539/23575

Downloaded from a DSpace repository. https://dspace.org/

Guest Editor's Introduction*: AJIC* Focus Section on Cybersecurity

Kiru Pillay
Visiting Researcher, LINK Centre, University of the Witwatersrand (Wits), Johannesburg; and Chief Director, Cybersecurity Operations, Department of Telecommunications and Postal Services, Pretoria

Abstract
This introduction to the *AJIC* Focus Section on Cybersecurity provides the context for the section, introduces the three articles, and establishes the importance of ongoing emperical research in support of policy and strategy in the cybersecurity domain.

Keywords
cybersecurity, cybersecurity policy, cyber-threats, cybersecurity awareness (CSA), cybersecurity research, developing world, Africa, South Africa

DOI: https://doi.org/10.23962/10539/23575

Recommended citation
Pillay, K. (2017). Guest editor's introduction: *AJIC* focus section on cybersecurity. *The African Journal of Information and Communication (AJIC)*, *20*, 79-82. https://doi.org/10.23962/10539/23575



This article is licensed under a Creative Commons Attribution 4.0 International (CC BY 4.0) licence: http://creativecommons.org/licenses/by/4.0

1. The widening range of cyber-threats

The imperative for developing countries to deploy information and communication technologies (ICTs) and the Internet as effective tools to redress historical challenges and inequalities is well understood by governments, nowhere more so than in Africa. ICTs and the Internet are seen as the essential channels to deliver a wide range of basic services and applications. This adoption of ICTs and the Internet into all aspects of everyday life has engendered emergence of what we refer to, in a favourable light, as information societies and knowledge economies.

However, the growth of such societies and economies is accompanied by new and serious threats. While technological advancement introduces greater variety and convenience into our lives, it also opens more and more avenues for people to be targeted by threat actors, who increasingly view public- and private-sector organisations – and individual citizens – as attractive targets for a range of cyber-threats.

Attacks against information infrastructure and Internet services are now commonplace, and 2017, in particular, has seen a large number of global incidents and data breaches. These attacks have placed the spotlight firmly on how governments are taking up the challenge of securing information systems, critical infrastructure and citizen's information, while at the same time building confidence in the ability to use the Internet to access services and transact safely. Numerous large-scale data breaches have released citizens' personal and financial information into the public domain and have, to a large extent, eroded confidence in the public and private sectors' abilities to defend against, and recover from, these attacks. These attacks have also increased the public's knowledge around issues like ransomware, with this word having now entered into daily usage. The scale and sophistication of the attacks are themselves increasing at a rate not seen previously, with cybercrime now emerging as a well-paid, outsourced model.

2. African cybersecurity responses

The issue of cybersecurity looms large in the strategies of many governments in Africa. Governments on the continent are increasingly mindful of the shared public-private responsibility for cybersecurity, and are aware of the need to mobilise both public and private organisations within a multistakeholder model. This is reflected in the growing number of African countries who have established, or are in the process of establishing, enabling policy and legislative frameworks for cybersecurity, including Botswana, Swaziland, Namibia and Zambia. Southern African Development Community (SADC) countries have been aided in the legislative drafting process by the development of SADC Computer Crime and Cyber Crime Model Laws, which are part of the Harmonisation of ICT Policies in Sub-Saharan Africa (HIIPSA) project. Continental instruments such as the African Union Convention on Cyber

Security and Personal Data Protection have also being mooted, and the ratification of this AU Convention is being actively pursued.

The key South Africa government response to the issue of cybersecurity has been passage of the National Cybersecurity Policy Framework (NCPF) in 2012, which is aimed at a "coherent and integrated Cybersecurity approach to address Cybersecurity threats", and at promotion of a cybersecurity culture and to building of confidence and trust in the secure use of ICTs (SSA, 2015). The NCPF has also given rise to the Cybercrimes and Cybersecurity Bill, which is currently before Parliament, and which will bring South Africa in line with international laws dealing with cybercrime (Minister of Justice, 2017).

The importance of cybersecurity is also reflected in the increasing number of countries that are establishing an operational capability in the form of national Computer Security Incident Response Teams (CSIRTs). These CSIRTs have a national mandate and currently exist in at least 16 African countries, with others either in the process of being established, or being planned. Apart from their domestic capabilities, national CSIRTs seek to address the transnational nature of cybersecurity incidents by developing cooperation frameworks between countries.

3. Contributions in this *AJIC* Focus Section

The three cybersecurity articles that follow in this *AJIC* Focus Section on Cybersecurity cover a broad spectrum of topics within the cybersecurity domain. The articles represent what is almost a hierarchy of issues and understandings that governments must have in order to create an enabling environment for cybersecurity. The first of these, covered in Sutherland's contribution, is the issue of governance and enabling policy and legislative frameworks. The article dissects the South African cybersecurity legislative ecosystem, and also delves into the issues of privacy and the operational capacity mandated by the legislative framework under the guise of national and sector CSIRTs.

The second article, by Van Niekerk, on cyber-incidents, provides a segue from the discussion of governance in encapsulating the range and scale of incidents faced by both the public and private sectors, and in describing the threat actors and the nature of the victims. The article illustrates why cybercrime is particularly difficult to combat, due to a range of factors including the ability of malicious actors to operate from anywhere in the world, the linkages between cyberspace and physical systems, and the difficulty of reducing vulnerabilities and consequences in complex cyber networks.

The third article, by Chandarman and Van Niekerk focuses on the issue of cybersecurity awareness (CSA). With humans now often cited as being the weakest

link in the cybersecurity value chain, the issue of CSA is high in the strategic plans of governments and private organisations. Awareness programmes are geared towards educating citizens around threats and vulnerabilities that exist in cyberspace and, in so doing, instilling in citizens a sense of confidence in their ability to transact and interact in cyberspace. But as this article demonstrates, there are elements of "cognitive dissonance" at play among users, making achievement of true CSA an extremely complex task.

4. Cybersecurity research

The need for research into the various aspects of cybersecurity is increasing and the current dearth of empirical data to inform policy and strategic interventions must be urgently addressed. Policy and strategic issues in the merging digital world are increasingly being conflated. Ownership of critical infrastructure by the private sector, and the threats posed to nation-states by any attack on this critical infrastructure, mean that multistakeholder approaches are imperative.

The sheer number of threat actors, and the principle that a threat actor need only be successful once, mean that the scale of the problem facing governments will only increase. The transnational nature of the incidents, and the increasing sophistication and technical capabilities of the threat actors facing government, mean that strategies and operational plans need to be as sophisticated and comprehensive as possible. Much more research will thus be required to inform these strategies and plans if they are to ensure that cyberspace is a predominantly safe place for interactions by individuals and institutions.

References

Minister of Justice (2017). *Cybercrimes and Cybersecurity Bill*. Minister of Justice and Correctional Services. Pretoria. Retrieved from http://www.justice.gov.za/legislation/bills/CyberCrimesBill2017.pdf

State Security Agency (SSA). (2015). *The National Cybersecurity Policy Framework (NCPF)*. Pretoria. Retrieved from https://www.gov.za/sites/www.gov.za/files/39475_gon609.pdf