The African Journal of Information and Communication (AJIC)
LINK Centre, University of the Witwatersrand (Wits)
Wits Tshimologong Digital Innovation Precinct
45 Juta St., Braamfontein 2001
Johannesburg, South Africa
www.wits.ac.za/linkcentre/ajic/

AJIC Call for Submissions: 2017 Thematic Section on Cybersecurity

The African Journal of Information and Communication (AJIC) is seeking submissions for a 2017 Thematic Section on Interdisciplinary Cybersecurity Studies.

Submission deadline: 30 April 2017

AJIC Corresponding Editor

- Dr Lucienne Abrahams, Director, LINK Centre, University of the Witwatersrand, Johannesburg

Guest Editors for the Thematic Section

- Dr Kiru Pillay, LINK Centre, University of the Witwatersrand, Johannesburg
- Dr Uche M. Mbanaso, Centre for Cyberspace Studies, Nasarawa State University, Keffi, Nigeria

Submissions: Submit to Dr Kiru Pillay: kiru2010@gmail.com

This *AJIC* Thematic Section will publish articles presenting original research in the interdisciplinary cybersecurity research domain. This call for academic contributions invites attention to a range of disciplines needed to understand the technological, economic, social and governance aspects of cybersecurity. This call invites articles within the following, broadly constructed and interpreted, aspects of cybersecurity:

Cybersecurity policy, legislation and regulation: Cybersecurity policies. legislation and regulation create an enabling environment for the formulation of cybersecurity strategies at both organisational and national levels. Models for effective regulation, monitoring of compliance, and monitoring of conformance are essential ingredients of cybersecurity and how it impacts national and regional economies.

Cyber-governance: Threat actors and threat vectors continue to evolve, even as the market, regulatory and legal tolerance for failure decreases. Cyber-governance relates to the frameworks by which policy or direction is provided, ensuring that the executive management of firms and entities, in the private sector, government and civil society, are aware and responsible for the security activities and can provide the assurance that actions and appropriate measures are being deployed. Governance is intended to increase the accountability of organisations and to avoid breaches and reputational damage. Cybersecurity is not just a technical issue but a business and governance challenge that includes risk management, reporting and accountability.

Social impact of cyber-risk: Today cyber threats affect the fabric of social life, as trust, confidentiality and privacy can be trampled upon as a result of cyber attacks. The ways in which cyber threats affect societies, cultures, religions and demographics may differ significantly in scope and severity.

Disruptive technologies in society: Continuous advances in digital technologies are transforming life, business, governance and the global economy. The procession of these novel technologies is emerging in many spaces, which includes the mobile Internet, autonomous vehicles and advanced genomics. Reshaping the world in which we live and work, digital technologies impact regions and even continents in often dissimilar ways, based on the socio-economic realities that are present. How leaders in government and business, and how citizens perceive the change and manage its impact on socio-economic development are important areas of study. This focus area includes issues of privacy and safety, cybersecurity awareness, and cybersecurity ethics and culture.

Big data, automation, analytics, artificial intelligence: Along with the concepts of big data, automation and artificial intelligence are the aligned issues of security, privacy and assurance. These emerging technologies, by their very nature, contain huge amounts of personal identifiable information (PII), as well as corporate data. Consequently, breaches to corporate information may lead to reputational damage, legal repercussions, and economic loss. This focus area includes secure big data analytic models and algorithms, security and risk assessments, secure distributed programming models, security best practices, secure data storage and audit logs, privacy-preserving models and architectures, granular access control architectures, secure cloud computing models, etc.

Internet of Things (IoT) and "smart everything": The IoT as a disruptive technology comes with intrinsic risks, like most other computing systems. The impact of IoT is evolving in multiple domains and contexts. Its applicability cuts across diverse human enterprises and the prediction is that it will grow well beyond what can be currently anticipated. It is likely to be more ubiquitous, implying the possibility for a variety of IoT devices to cooperate, collaborate, or share information, even when they are unlikely to belong to a single (or the same autonomous) security domain. Security and safety are therefore paramount and besides the issues of confidentiality, integrity and availability lies the issues of trust and privacy. This focus area includes pervasive security architectures, risk, threat and vulnerability assessments, safety assessment and requirements, impact on socio-economic values, as well as governance issues.

Cybersecurity strategic frameworks, maturity models, architectures: This focus area includes security issues relating to critical information infrastructure protection (CIIP), risk assessment and management, resilience maturity measurement models, and country specific experiences in national efforts relating to adoption and acceptance, sectoral or organisational perspectives.

Guest Editors' note: Many information security and cybersecurity conferences, seminars and workshops take place on the African continent on an annual basis. The above mentioned topics were discussed at, among others, the 2016 Africa Internet Summit (AIS 2016) convention and training event in Botswana in May-June 2016, Africa Cyber Security Summit in 2016 in Johannesburg, the 2016 BSideLagos Cyber-Security Conference in Nigeria and the South African Reserve Bank Cyber Security Conference, with a particular emphasis on the increasing cybersecurity threats and trends, as well as countermeasures. Enhanced or extended papers arising from these conferences and workshops are especially invited for consideration in this forthcoming thematic issue of the *AJIC.*

This focus aligns with *AJIC*'s concern with Africa's participation in the information society, and its focus on disseminating original research on digital technology issues at the global, regional and national level that have implications for developing countries in general, and for Africa and the Southern African region in particular. For previous issues of the journal, please go to *AJIC*.

Key submission guidelines: Contributions are hereby invited for consideration for inclusion in the Thematic Section. Prior to selection for inclusion, submissions will be subject to double-blind peer review and must meet the publication standards and editorial requirements of *AJIC*. Authors are expected to implement appropriate revisions and extensions to the original submission, including revisions advised by the peer reviewers. Unpublished conference papers will also be considered for publication. Full-length articles and conference paper submissions should be ±6,000 words. Shorter contributions in the form of thematic reports, book reviews, theoretical reflections, case notes of research in progress, and other scholarly items, will also be considered for review. These contributions should be ±2,500-3,000 words. Please see the detailed ***AJIC* Submission Guidelines.**

Referencing: *AJIC* follows the APA referencing style. Authors can familiarise themselves with APA style at **www.apastyle.org**, noting, in particular, the online tutorial and blog.