PO Box 1560, Parklands, 2121 • Tel +2711 788 1278 • Fax +2711 788 1289
Email info@mma.org.za • www.mediamonitoringafrica.org
Promoting human rights and democracy through the media since 1993

8 August 2017
19 Pages

TO: PORTFOLIO COMMITTEE ON JUSTICE AND CORRECTIONAL SERVICES
C/O Mr V Ramaano
E-mail: vramaano@parliament.gov.za
Due date: 10 August 2017

WRITTEN SUBMISSIONS ON THE CYBERCRIMES AND CYBERSECURITY BILL [B6-2017] SUBMITTED BY MEDIA MONITORING AFRICA (MMA), AND SUPPORTED BY MEDIA 24 AND KAGISO MEDIA

For more information please contact:

WILLIAM BIRD, *Director of MMA*
E-mail: williamb@mma.org.za
Tel: +2711 788 1278

MMA was assisted in the drafting of these written submissions by Applied Law & Technology:
https://altadvisory.africa

CONTENTS

LIST OF ACRONYMS

CAB	Copyright Amendment Bill [B13-2017]
CCB	Cybercrimes and Cybersecurity Bill [B6 – 2017]
DPME	Department of Planning, Monitoring and Evaluation
ECTA	Electronic Communication and Transactions Act 25 of 2002
FPB	Films and Publications Amendment Bill [B37-2015]
ISC	Interdepartmental Steering Committee
MMA	Media Monitoring Africa
OECD	Organisation for Economic Co-Operation and Development
POPI	Protection of Personal Information Act 4 of 2014
SEIAS	Socio Economic Impact Assessment System

SUMMARY OF WRITTEN SUBMISSIONS

Media Monitoring Africa (MMA) is a non-profit organisation that promotes democracy and a culture where media and the powerful respect human rights and encourage a just and fair society. MMA welcomes the invitation by the Portfolio Committee on Justice and Correctional Services to make written submissions on the Cybercrimes and Cybersecurity Bill [B6-2017] (CCB). MMA would also welcome the opportunity to make oral submissions and hereby requests that when these occur MMA is afforded an opportunity to make such submissions.

MMA's written submissions are divided into two broad categories: (1) overall impressions of the CCB and structural concerns; and (2) specific concerns with the CCB. Within these two broad categories MMA makes eight recommendations (***see page 18***).

This submission is supported by Media 24 and Kagiso Media.

Overall impressions of the CCB and structural concerns

As a point of departure, MMA's primary concern about the current CCB is ***the lack of any overarching internet governance policy***, that MMA has seen, on how current and proposed legislation – including the CCB – which deal with how information and digital rights (freedom of expression, access to information, and privacy) regulation is to be managed. In this regard, MMA proposes the establishment of an Interdepartmental Steering Committee (ISC) or other overarching internet governance management node within the state as a necessary – and, arguably, constitutionally required – response to bring harmony to South Africa's internet governance framework and to ensure swift and effective state responses to cybercrimes and other related concerns. The ISC may be aligned and structured in accordance with the Cyber Response Committee as outlined below, which may be well-suited as a sub-committee of the ISC (***see page 7***).

Further, MMA has neither had sight of any ***impact assessment for the CCB completed by the Socio-Economic Impact Assessment System (SEIAS) Unit*** established by the Cabinet, nor has it been made aware that an impact assessment has been completed and made publicly available. Given the complexities with internet governance, MMA is of the view that if an impact assessment has been completed, it should be made public without undue delay and stakeholders should be permitted the opportunity to make submissions on the impact assessment. In the event that an impact assessment has not been completed, further deliberations on the CCB should be halted until such time as stakeholders and members of Parliament have had the opportunity to consider, and the public has had the opportunity to provide submissions on, ***the socio-economic impacts of the CCB*** (***see page 10***).

Specific concerns with the CCB

In summary, MMA has concerns about the absence of reference to children in the CCB; the possible overreach of certain sections on malicious communications; the composition of the Cyber Response Committee; the scope of certain sections on critical information infrastructure; and the absence of appropriate pubic interest considerations.

MMA takes the view that the ***protection of the best interests of the child*** in cybercrimes and cybersecurity should, at a minimum, be acknowledged in the CCB. In this regard, MMA proposes that sub-sections which refer to the protection of children be included in sections 16 to 18 of the current CCB. Alternatively, a new section should be drafted dealing with criminal sanctions relating to the exposure of children to pornography, the use of technology to groom and exploit children, and the need to develop appropriate curricula (***see page 11***).

In terms of ***malicious communications***, MMA is concerned that the CCB unduly restricts -- and may have a chilling effect on -- the right to freedom of expression, and that it creates disunity between criminal laws online and offline. MMA therefore recommends, at a minimum, redrafting the definition of a harmful data message and expanding on the definition of property in section 17(2)(a); amending section 17(2)(c) to replace "intimidates, encourages or harasses" with "incites"; deleting section 17(2)(d), pending further investigation by the proposed ISC; and inserting the requirement of harm into section 18 (***see page 12***).

With regards to the ***composition of the Cyber Response Committee***, MMA is concerned that oversight of the Committee is exercised by the Minister of State Security and suggests that such oversight should rest with the Minister of Justice and Correctional Services. Further, MMA is concerned that there are no independent members on the Committee, outside of state functionaries, and proposes a structure similar to that of the constitutionally-mandated Judicial Services Commission (***see page 13***).

In terms of ***critical information infrastructure***, MMA suggests the drafting of a more comprehensive definition of "information infrastructure" and the establishment of an independent authority, such as an ombudsman, to review declarations of critical information infrastructure, particularly where the information infrastructure is owned by, among others, the media, civil society organisations and / or non-governmental organisations, or human rights defenders (***see page 17***).

Finally, MMA recommends that in order to enable the protection and promotion of the right to freedom of expression, the CCB should include a ***public interest defence*** to malicious communications, which will ensure that members of the media, human rights defenders and other members of the public can hold public officials and powerful individuals accountable without fear of sanction (***see page 17***).

INTRODUCTION

1. Media Monitoring Africa[1] (MMA) welcomes the invitation to submit written submissions on the Cybercrimes and Cybersecurity Bill [B6 – 2017] (CCB) from the Portfolio Committee on Justice and Correctional Services (Portfolio Committee). These written submissions are made in accordance with that invitation, and are supported by Media 24[2] and Kagiso Media.[3]

2. MMA commends the Portfolio Committee for its continuing work on the CBB and some of the welcome amendments which have been made following the written submissions of MMA dated 30 November 2015, and others, on the 2015 Bill. Particularly, MMA acknowledges the deletion of the sections relating to copyright in the 2015 Bill.

3. In terms of this invitation – and alongside these written submissions – **MMA requests an opportunity to make a verbal presentation during this round of public hearings on the CCB**.

About Media Monitoring Africa

4. MMA is a non-profit organisation that promotes democracy and a culture where media and the powerful respect human rights and encourage a just and fair society. MMA acts in a watchdog role to promote ethical and fair journalism that supports human rights.

5. MMA's vision is a just and fair society empowered by a free, responsible and quality media. Through a human rights-based approach, MMA aims to promote the development of:

    5.1. Media that is transparent, diverse, ethical and accountable to its audiences;
    5.2. Critical and constructive communications by the powerful; and
    5.3. Informed, engaged and connected citizenry.

6. MMA aims to contribute to this vision by being the premier media watchdog in Africa to promote a free, fair, ethical and critical media culture. MMA has over 20 years' experience in media monitoring and direct engagement with media, civil society organisations and citizens. MMA is the only independent organisation that analyses and engages with media according to this framework. In all of its projects, it seeks to demonstrate leadership, creativity and progressive approaches to meet the changing needs of the media environment.

[1] For more information about MMA, see: http://www.mediamonitoringafrica.org/index.php/about/. MMA was assisted in the drafting of this submission by Applied Law & Technology (Pty) Ltd: https://altadvisory.africa
[2] For more information about Media 24, see: http://www.media24.com/about/
[3] For more information about Kagiso Media, see: http://kagisomedia.co.za/who-we-are/

7. Increasingly, cybercrimes and cybersecurity are becoming central to the changing needs of the media environment and thus fall squarely within the mandates of MMA, Media 24 and Kagiso Media.

OVERALL IMPRESSIONS OF THE CCB AND STRUCTURAL CONCERNS

8. MMA is aware that, at present, South Africa has no legislation that directly addresses cybercrimes and cybersecurity. The CCB therefore remains timeous in that it seeks to propose a legislative framework that brings South Africa in line with foreign and international laws governing internet-based crimes. Following the amendments to the 2015 Bill, MMA commends the Portfolio Committee on its work in remedying sections that may have been interpreted as constitutionally impermissible. However, the current CCB, in MMA's view, may still fall foul of South Africa's constitutional framework.

The need for an Interdepartmental Steering Committee (ISC)

9. Primary to MMA's concerns about the current CCB is the lack of any overarching internet governance policy, that MMA has seen, on how current and proposed legislation -- including the CCB – which deal with how information and digital rights (freedom of expression,[4] access to information,[5] and privacy[6]) regulation is to be

[4] Section 16 of the Constitution provides:

"Freedom of expression

16. (1) Everyone has the right to freedom of expression, which includes—
    (a) freedom of the press and other media;
    (b) freedom to receive or impart information or ideas;
    (c) freedom of artistic creativity; and
    (d) academic freedom and freedom of scientific research.
    (2) The right in subsection (1) does not extend to—
    (a) propaganda for war;
    (b) incitement of imminent violence; or
    (c) advocacy of hatred that is based on race, ethnicity, gender or religion, and that constitutes incitement to cause harm."

[5] Section 32 of Constitution provides, in part:

"Access to information

32. (1) Everyone has the right of access to—
    (a) any information held by the state; and
    (b) any information that is held by another person and that is required for the exercise or protection of any right."

[6] Section 14 of the Constitution provides:

"**Privacy**

14. Everyone has the right to privacy, which includes the right not to have—
    (a) their person or home searched;
    (b) their property searched;

managed. As dealt with below, MMA has also not had sight of any SEIAS impact assessment on the CCB and is therefore uncertain as to how current and proposed legislation is to be coordinated within the state, and what impacts the various pieces legislation may have on people in South Africa. Further, MMA remains uncertain as to how coordination of various internet governance bodies, such as the Cyber Response Committee and the National e-Strategy[7] will be effected.

10. Alongside the CCB, the Prevention and Combating of Hate Crimes and Hate Speech Bill [2016] (Hate Crimes and Hate Speech Bill), the Films and Publications Amendment Bill [B37-2015] (FPB), the Copyright Amendment Bill [B13-2017] (CAB), the Protection of Personal Information Act 4 of 2014 (POPI), and the National E-Strategy in terms of the Electronic Communication and Transactions Act 25 of 2002 (ECTA), among others, all contain sections relevant to internet governance but do not expressly indicate how interdepartmental cooperation is going to occur for the purposes of overall internet governance policy within the state. In the absence of a clear government internet governance policy and legislative guidance, an unduly complex structure of oversight is in the process of being created.

11. It is now commonly acknowledged that there are regulatory difficulties associated with technology innovation,[8] and that information rights continue to be defined and developed in the digital age. The OECD suggests that "regulatory reform is directed to making sure that regulations are fully responsive to changes in the economic, social and technical conditions surrounding them".[9] MMA's central concern, in the absence of guidance from the SEIAS Unit and a clear and publicly accessible overarching internet governance policy, is that people in South Africa, civil society organisations, and members of the media, among others, need to navigate an overly complex regulatory landscape in order to make submissions, conduct their business, and, ultimately, defend and protect their information rights. Additionally, this poses significant challenges to government's coordinated and effective implementation of the existing regulatory provisions, and may result in overlapping mandates or aspects not being assigned or accounted for by appropriate functionaries.

12. Further, with rapid technological developments, including the development of technologies used to perpetrate cybercrimes, the complex governance structures

(c) their possessions seized; or
(d) The privacy of their communications infringed."

[7] Department of Telecommunications and Postal Services, *National E-Strategy: Technology Working for the People to Build an Information and Knowledge Society* (7 April 2017): https://www.dtps.gov.za/images/phocagallery/Popular_Topic_Pictures/National-e-strategy.pdf
[8] See, for example, Organisation for Economic Co-Operation and Development (OECD), *Regulatory Reform and Innovation*: https://www.oecd.org/sti/inno/2102514.pdf
[9] Id at page 7.

created by the various pieces of legislation dealing with internet governance may not be amenable to swift and effective responses to cybercrimes and technological developments by the state which, in turn, may lead to a derogation by the state of its constitutional obligation to respect, protect, promote and fulfil the rights in the Bill of Rights,[10] including all of the listed information rights. A further constitutional consideration relates to cooperative governance and intergovernmental relations. In terms of section 41(1)(c) of the Constitution "[a]ll spheres of government and all organs of state within each sphere must provide effective, transparent, accountable, and coherent government for the Republic as a whole" and the must "co-operate with one another in mutual trust and good faith by coordinating their actions and legislation with one another".[11]

13. To the extent that an overarching internet governance policy and a central node within the state is not established to manage internet governance – for example, through the establishment of an ISC on Internet Governance which coordinates all of the regulatory efforts of the state detailed above – the possibility of a series of legal challenges exists, which, in turn, may cause the state to not only potentially violate information rights but also the cooperative governance principle that all spheres of government must avoid legal proceedings against one another.[12]

14. We note the establishment of the Cyber Response Team under Chapter 10 of the CCB, which we deal with in more detail below. The composition of the ISC may build on the structure proposed for the Cyber Response Team, supplemented with other functionaries relevant to internet governance, as the mandate of the ISC would be broader than that of the Cyber Response Team. Structurally, it may be suitable to house the Cyber Response Team as a sub-committee of any such ISC.

15. With this said, MMA fully appreciates the complexities associated with regulating a rapidly expanding technological environment and commends the various organs of state for their current efforts. However, MMA is of the view that the establishment of an ISC or other overarching internet governance management node within the state is a necessary – and, possibly, constitutionally required -- response to bring harmony to South Africa's internet governance framework and to ensure swift and effective state responses to cybercrimes. Specifically, MMA proposes that within the proposed ISC or other overarching internet governance management node, and in addition to state functionaries, a variety of stakeholders, including independent experts and representatives of civil society, should be included in the proposed structure to ensure

[10] See section 7(2) of the Constitution.
[11] See section 41(1)(h)(iv) of the Constitution.
[12] Section 41(1)(h)(vi) of the Constitution.

coherence, good governance, and that the requisite support is provided to decision-makers.[13]

Socio-Economic Impact Assessment System (SEIAS)

16. Following the establishment of the SEIAS by the Cabinet in February 2007, from 1 October 2015 any Cabinet Memoranda seeking approval for draft policies, bills, or regulations must include a socio-economic impact assessment compiled and approved by the SEIAS Unit.[14] The SEIAS, which replaces the Regulatory Impact Assessment, aims to "minimise unintended consequences from policy initiatives, regulations and legislation, including unnecessary costs from implementation and compliance as well as from unanticipated outcomes", and "to anticipate implementation risks and encourage measures to mitigate them".[15] At this stage, MMA has neither had sight of any impact assessment for the CCB, nor has it been made aware that an impact assessment has been completed and made publicly available.

17. In terms of the *SEIAS Guidelines*, the system applies to "new or to be amended primary legislation, although the impact assessment need not be published for matters affecting national security."[16] MMA is of the view that the CCB's central aim is far broader than the protection of national security and therefore an impact assessment needs to be conducted and made public. More so, with the complexities detailed above, stakeholders may be well placed to further assist the state with crafting an appropriate internet governance framework and avoiding unintended consequences.

18. MMA is of the view that if an impact assessment has been completed, it should be made public without undue delay and stakeholders should be permitted the opportunity to make submissions on the impact assessment. MMA is concerned that the public is yet to have sight of the impact assessment, which, in this context, is a self-imposed Cabinet obligation and a necessary tool in better understanding internet governance proposals within the state. In the event that an impact assessment has not been completed, further deliberations on the CCB should be halted until such time as stakeholders and members of Parliament have had the opportunity to consider, and the public has had the opportunity to provide submissions on, the socio-economic impacts of the CCB.

[13] See paras 30-7 below.
[14] Department of Planning, Monitoring and Evaluation, *Socio-Economic Impact Assessment System (SEIAS): Guidelines* (May 2015) at page 3: http://www.dpme.gov.za/keyfocusareas/Socio%20Economic%20Impact%20Assessment%20System/SEIAS%20Documents/SEIAS%20guidelines.pdf
[15] Id at page 4.
[16] Id at page 8.

SPECIFIC CONCERNS WITH THE CCB

19. Outside of the overarching concerns around internet governance and interdepartmental cooperation detailed above, MMA has specific concerns about the absence of reference to children in the CCB; the possible overreach of certain sections on malicious communications; the composition of the Cyber Response Committee; the scope of certain sections on critical information infrastructure; and the absence of appropriate pubic interest considerations.

The best interests of children are not considered

20. As detailed in its written submissions on the 2015 Bill, MMA remains concerned that the CCB does not appropriately consider the best interests of children, the use of technology to exploit children, and the current levels of digital literacy in South Africa. By way of an example, the CCB does not once mention "children" or "child", save for in the schedule of "Law Repealed or Amended". Given that South Africa has one of the most progressive constitutions in the world, especially with regards to the rights of children, and provides that "[a] child's best interests are of paramount importance in every matter concerning the child",[17] it is imperative that the best interest of the child, particularly in online spaces, are addressed by the CCB.

21. We note in this regard that the concerns are effectively two-fold. In the first instance, we are concerned with the possibility of children falling foul of the provisions under the CCB, and being subject to criminal sanctions as a result of their immaturity and/or lack of understanding of the import of the CCB. We submit that it is necessary for the CCB to contemplate an appropriate dispensation for children who may be in breach of the CCB. Coupled with this, it is important for there to be appropriate education and training for children on the impact of the CCB, as well as other pieces of legislation that may impact children and their expression online, in order to ensure they are aware of the potential consequences. In this regard, the proposed ISC or other overarching internet governance management node is well placed to consider educational approaches, including curricula development, to ensure the safety and security of children online, including the impact of cybercrimes – particularly cyber-bullying and cyber-harassment -- on children

22. Second, MMA persists with its position that the CCB does not have appropriate regard to the exposure of children to pornography and the use of technology to groom and exploit children, in the light of the *South African Law Reform Commission Project on*

[17] Section 28(2) of the Constitution provides that "[a] child's best interests are of paramount importance in every matter concerning the child".

Sexual Offences: Pornography and Children.[18] While MMA acknowledges the efforts by the Department of Justice and Correctional Services to amend the Criminal Law (Sexual Offences and Related Matters) Amendment Act 32 of 2007, MMA takes the view that the protection of the best interests of the child in cybercrimes and cybersecurity should, at a minimum, be acknowledged in the CCB.

23. In this regard, MMA proposes that sub-sections be included in sections 16 to 18 of the current CCB to address the appropriate dispensation for children who contravene the CCB, the need for education and training particularly for children, and which make reference to the protection of children. Alternatively, a new section should be drafted dealing specifically with concerns relating to children.

Malicious communications and freedom of expression (sections 16, 17, and 18)

24. As an overarching principle, MMA remains concerned with the conflation of various pieces of legislation – including the Protection from Harassment Act 17 of 2011, the Hate Crimes and Hate Speech Bill, the proposed repeal of sections 85, 86, 87, 88 and 90 of the ECTA, the CCB, and the common law – and the limited reference to information rights, including the constitutional right to freedom of expression[19] in the various preambles or elsewhere. Additionally, MMA is concerned that the CCB does not adequately acknowledge that information rights are equally as applicable online as they are offline, a position recently restated by the United Nations Human Rights Council.[20] MMA submits that information rights, and their applicability in the cybercrimes and cybersecurity framework, need to be properly considered in the CCB.

25. With regard to section 17(2)(a)(i), the reference to "any property" does not consider the possibly different thresholds for movable, immovable, and, increasingly, virtual property such as one's brand or intellectual property online. MMA further proposes the insertion of the word "imminent" before all references to violence in sub-sections 17(2)(a) and (b).

26. With regard to section 17(2)(c) of the CCB, MMA notes that the CCB ought to be brought in line with existing laws relating to such offences. Specifically, MMA proposes replacing the words "intimidates, encourages or harasses" with the word "incites".

27. Of particular concern to MMA is that the CCB seeks to introduce a new limitation on free speech in section 17(2)(d) which makes it a criminal offence to distribute a harmful

[18] South African Law Reform Commission, Project 107, Issue Paper 30, *Sexual Offences: Pornography and Children* (5 August 2015): http://salawreform.justice.gov.za/ipapers/ip30_prj107_SexualOffences-PC-2015.pdf
[19] See note 4 above.
[20] United Nations Human Rights Council Resolution 32/13 (18 July 2016), A/HRC/RES/32/13: ap.ohchr.org/documents/dpage_e.aspx?si=A/HRC/RES/32/13

data message that is inherently false. In this instance, the distribution of a harmful message online will carry a criminal sanction which does not necessarily exist offline, and, as such, creates disunity between criminal laws in online and offline spaces. While this provision appears to be a response to concerns regarding so-called 'fake news', such a provision would be a severe limitation on the right to freedom of expression, and would arguably not be justifiable under section 36 of the Constitution whether applied online or offline. In our view, such a provision is inapposite in the CCB, and should instead be a matter to be dealt with by the ISC proposed above in the appropriate forum.

28. As a general comment relating to sections 16, 17 and 18, MMA is concerned by potential unintended consequences that these provisions could have on the enjoyment of freedom of expression given their broad and far-reaching ambit. For instance, section 18 does not require the element of harm and thus leads to the possible absurdity of the criminal prosecution of a parent who shares a nude picture of a new born baby with family members. While such an example may be unlikely to lead to a prosecution, the concern is that these provisions may be selectively used and will have a chilling effect on the right to freedom of expression. As such, MMA urges the drafters to carefully consider the impact of these provisions, and ensure that the provisions are carefully and narrowly circumscribed in order to avoid ambiguity.

29. Accordingly, MMA recommends, at a minimum, redrafting the definition of a harmful data message as outlined above; expanding on the definition of property in section 17(2)(a); inserting the word "imminent" before "violence" in section 17(2)(a) and (b); replacing the words "intimidates, encourages or harasses" with "incites" in section 17(2)(c); deleting section 17(2)(d), pending further investigation by the proposed ISC; and inserting the requirement of harm into section 18. Alternatively, as a result of the introduction of the Hate Crimes and Hate Speech Bill and the need to avoid the conflation of laws detailed above, MMA proposes the deletion of sub-sections 17(2)(c) and (d) from the CCB.

Composition of the Cyber Response Committee (section 53)

30. In terms of section 53 of the CCB, the Cyber Response Committee (Committee), which is responsible for the implementation of government policy relating to cybersecurity is established.[21] The CCB further provides that the Cabinet member responsible for State Security is mandated to oversee and exercise control over the performance of the functions of the Committee.[22] In terms of its operations, the Committee consists of a Chairperson, who is the Director-General: State Security, and two members of

[21] Section 53(5).
[22] Section 53(6).

"representative" departments, including the Head of Department.[23] MMA has three concerns with the establishment of the Committee:

30.1. MMA is concerned that oversight of the Committee is exercised by the Minister of State Security. No motivation as to why this should be the case is provided, and given the general focus of the issues the CCB seeks to deal with, it seems at odds with both the intent and purpose of the CCB for oversight of the Committee to be controlled by the Minister of State Security. This is not to suggest that there are not circumstances in which matters of state security may be paramount.

30.2. MMA suggests that control of the Committee should rest with the Minister of Justice and Correctional Services; and

30.3. MMA is concerned that there are no independent members on the Committee, outside of state functionaries, and proposes a structure similar to that of the constitutionally-mandated Judicial Services Commission.[24]

The Minister of Justice should exercise control over the Committee

31. Notwithstanding the potential threats to national stability, the constitutional order, and the safety and wellbeing of people in South Africa, cybercrimes policy and the management of the Committee may be more effective if it is located under the control of the Minister of Justice and Correctional Services, and administered by the Director-General: Justice as the Chairperson. This is so because the Department of Justice and Correctional Services has a less direct role in investigating and engaging in cybercrimes under the CCB – unlike the State Security Agency,[25] the South African Police Service,[26] the South African National Defence Force,[27] and the Department of Telecommunications and Postal Services.[28]

32. Accordingly, the Minister of Justice and Correctional Services and the relevant Director-General may be more impartial in their oversight function, and will be competently

[23] In terms of section 53(8)(b) of the CCB, "representative Department" means: the Department of Defence; the Department of Home Affairs; the Department of International Relations and Cooperation; the Department of Justice and Constitutional Development; the Department of Science and Technology; the Department of Telecommunications and Postal Services; the Financial Intelligence Centre; the National Prosecuting Authority; the National Treasury; the South African Police Service; the South African Reserve Bank; the South African Revenue Service; the State Security Agency; and any other Department requested by the Chairperson.
[24] See section 178 of the Constitution.
[25] See section 54(1).
[26] See section 54(2).
[27] See section 54(3).
[28] See section 54(4).

assisted by the Committee, which will include the various Ministers in the so-called security cluster and the additional independent members of the Committee proposed below. In this instance, government cybersecurity policy may be facilitated through public participation as opposed to primary reliance on securitisation, intelligence gathering, and defence. Given the wide-ranging impact and role that the CCB will have, we submit that the Minister of Justice and Correctional Services is best-placed to take a broad view of the overall effect and inter-related considerations that will arise.

Membership of the Committee

33. Currently, the CCB makes provision for approximately 30 members of the Committee, of which three members are from the State Security Agency, and all members are Heads of Department or nominees of the Heads of Departments. MMA is concerned that this is unwieldy and impracticable, particularly for a Committee that may be required to respond to immediate and time-sensitive threats. The broad membership of the Committee may be better-suited to the proposed ISC, with a smaller composition for the Committee itself. This may be achieved by reducing the number of representatives of each department and/or reducing the number of departments.[29]

34. However, in MMA's view, it is critical that the Committee and the ISC are represented by a diversity of views, which we submit is both constitutionally permissible, and necessary to manage increasing and rapid developments in cybersecurity.

35. Accordingly, relying partially on the structure of the Judicial Services Commission in section 178 of the Constitution, MMA suggests that the membership of the Committee and the proposed ISC should include, in addition to departmental representatives and representatives of organs of state, the following members:

    35.1. Representatives from opposition parties represented in the National Assembly;
    35.2. *Two* teachers of law, or members of the attorneys' or advocates' profession, with knowledge of cybersecurity-related laws who are approved by the Chairperson of the Committee following a public call for nominations.
    35.3. *Two* technical experts in cybersecurity who are approved by the Chairperson of the Committee following a public call for nominations.
    35.4. *Two* members of civil society organisations working on cybersecurity policy who are approved by the Chairperson of the Committee following a public call for nominations.

[29] See para 36 below.

36. In terms of the above proposal, the Committee will comprise approximately 38 members. However, in the event that section 53(8)(b) of the CCB is amended to include only one member from each department and organ of state, representation on the Committee can be reduced to 24 members. In the event that the membership of representatives of organs of state (excluding departmental representatives) is deleted from section 53(8)(b) of the CCB and the membership of representatives of organs of state is reserved for the proposed ISC, representation on the Committee can be further reduced to approximately 16 members, a position that MMA supports due to the need immediate and time-sensitive response to cybersecurity threats.

37. Given the national importance of cybersecurity policy in an increasingly challenging regulatory space, MMA is of the view that the additional proposed members to the Committee, including those with direct technical expertise, will assist the Chairperson of the Committee establish an effective and responsive government cybersecurity policy going forward.

Critical Information Infrastructure (section 57)

38. In terms of critical information infrastructure, MMA persists with the concerns that it raised in its written submissions on the 2015 Bill. MMA remains particularly concerned with the circular and broad definition of "information infrastructure",[30] which plausibly could include almost anything related to a computer or information communications technology, including all buildings containing any form of network.

39. Further, MMA remains concerned that in terms of section 57(3)(i), the Minister of State Security can declare an information structure belonging to "a company, an entity or a person", a critical information infrastructure. This sub-section clearly includes, among others, media houses and independent media providers, civil society organisations and non-governmental organisations, journalists, and human rights defenders. In the absence of clear legislative guidance on the content of the "directives" that the Minister may issue to owners of a critical information infrastructure in terms of section 57(4), particularly the "classification of data held",[31] this sub-section may violate information rights, particularly the rights to freedom of expression and privacy.

40. To remedy the concerns, MMA suggests the drafting of a more comprehensive definition of "information infrastructure" and the establishment of independent authority, such as an ombudsman, to review declarations of critical information

[30] Section 57(2) of the CCB states, in part, that "[t]he Cabinet member responsible for State security may . . . declare any information infrastructure, or category or class of information infrastructures, or any part thereof, as critical information structures".
[31] See section 57(4)(a).

infrastructure, particularly where the information infrastructure is owned by, among others, the media, civil society organisations and / or non-governmental organisations, or human rights defenders.

Public interest considerations

41. In terms of public interest considerations and with reference to MMA's written submissions on malicious communications above, MMA submitted in its written submission on the 2015 Bill that there needs to be a "deliberative move towards protecting intention [for the purposes of malicious communications or disclosure] that is in the public interest."[32]

42. The current version of the CCB makes no reference to communications, intentionally made available, broadcast, or distributed which are in the public interest, the interest of justice, or already in the public domain. The chilling effect of this omission is that journalists or human rights defenders who publish malicious communications, which may be in the public interest or in the interest of justice, are still criminally liable in terms of the CCB. To enable the protection and promotion of the right to freedom of expression, the CCB should include a public interest defence to malicious communications, which will ensure that public officials and powerful individuals can be held accountable by members of the media and human rights defenders.

CONCLUSION

43. MMA appreciates the ongoing work of the Department of Justice and Constitutional Development on the CCB, and it acknowledges the complexities with regulating cybercrime. However, MMA takes the view that the CCB, in its current form and in the absence of remedying the sections detailed above, does not provide an adequate, holistic, and constitutionally compliant response to cybercrimes and cybersecurity in South Africa.

44. MMA makes itself available to further assist Parliament and the Department of Justice and Correctional Services in its continuing efforts to develop an appropriate and responsive cybersecurity policy and legislative framework.

[32] Media Monitoring Africa, *Written Submissions by Media Monitoring Africa (MMA) on the Cybercrimes and Cybersecurity Bill (Draft for Public Comment)* (20 November 2015) at page 7.

SUMMARY OF RECOMMENDATIONS

- An ISC or other overarching internet governance management node within the state is a necessary – and, possibly, constitutionally required -- response to bring harmony to South Africa's internet governance framework and to ensure swift and effective state responses to cybercrimes.

- MMA has not had sight of an impact assessment by the SEIAS Unit. If an impact assessment has been completed, it should be made public without undue delay and stakeholders should be permitted the opportunity to make submissions on the impact assessment. In the event that an impact assessment has not been completed, further deliberations on the CCB should be halted until such time as stakeholders and members of Parliament have had the opportunity to consider, and the public has had the opportunity to provide submissions on, the socio-economic impacts of the CCB.

- MMA proposes that sub-sections which make reference to the protection of children be included in sections 16 to 18 of the current CCB. Alternatively, a new section is drafted dealing with criminal sanctions relating to the expose of children to pornography, the use of technology to groom and exploit children, and the need to develop curricula informing children about cybercrimes.

- Sections 16 to 18: At a minimum, the definition of a harmful data message and the definition of property in section 17(2)(a) should be redrafted; sub-sections 17(2)(c) should be amended to replace "intimidates, encourages or harasses" with "incites"; section 17(2)(d) should be deleted, pending further investigation by the proposed ISC; and the requirement of harm should be inserted into section 18.

- Section 53(2): The current membership of the Cyber Response Committee should be amended to ensure that it is able to function quickly and effectively, and should include members of the opposition represented in the National Assembly; two teachers of law, or members of the attorneys' or advocates' profession, with knowledge of cybersecurity-related laws; two technical experts in cybersecurity; and two members of civil society organisations working on cybersecurity policy.

- Section 53(5): The Cabinet member responsible for the Department of Justice and Correctional Services, as opposed to the Cabinet member responsible for State Security, should oversee and exercise control over the performance of the functions of the Cyber Response Committee.

- Sections 57(2) to (4): A more comprehensive definition of "information infrastructure" needs to be drafted and an independent authority, such as an ombudsman, should be

established by the CCB to review declarations of critical information infrastructure, particularly where the information infrastructure is owned by, among others, the media, civil society organisations and / or non-governmental organisations, or human rights defenders.

- To enable the protection and promotion of the right to freedom of expression, the CCB should include a public interest defence to malicious communications, which will ensure that public officials and powerful individuals can be held accountable by members of the media and human rights defenders.

MEDIA MONITORING AFRICA
Johannesburg, 8 August 2017

ENDS.