Submission on the

Cybercrime and Cybersecurity Bill

Attention:

SJ Robbertse

Ministry of Justice and Correctional Services

SALU Building

28th Floor, 316 Thabo Sehume Street

Pretoria

South Africa

Email: cybercrimesbill@justice.gov.za

14 December 2015

For further information please contact:

Research ICT Africa

info@researchictafrica.net

Telephone +27 21 447 6332. Fax +27 21 447 9529

Research ICT Africa welcomes this opportunity to comment on the Cybercrime and Cybersecurity Bill – Draft for Public Comment (hereinafter Draft Bill) released by the Minister of Justice and Constitutional Development on 28 August 2015.

Research ICT Africa is a regional ICT policy and regulation think tank active across Africa and the Global South. The think tank conducts research on ICT policy and regulation that facilitates evidence-based and informed policy making for improved access, use and application of ICT for social development and economic growth.

We make this submission in the public interest to ensure that a Cybercrime and Cybersecurity Bill is drafted with the intention of protecting Internet users' rights to safety and security, privacy, access to information, and freedom of expression and information. We strongly believe that internet users can benefit from a safe a secure access and use of the Internet. We also believe that in terms of the Universal Declaration of Human Rights and the International Covenant on Civil and Political Rights the State has a duty to protect the civil, political, economic, social and cultural rights of its citizens, which in South Africa are enshrined in its Constitution, offline and online.

While noting national rights and responsibilities, this submission draws attention to the fact that the internet remains a global and decentralised network governed by decentralised multistakeholder governance structures and processes; that public decisions affecting how the internet is governed are taken through the involvement of all stakeholders affected by such decisions; and that an evidence-based approach to policy and regulation development is likely to produce the best outcomes in policy formulation.

We thank the Minister of Justice and Constitutional Development for instituting a public process to determine a framework for the governance of cybercrime and cybersecurity, privacy protection, access to information, copyright protection, and freedom of expression, and to promote the idea that a safe and secure internet is a matter of public interest which involves all South African citizens, the public and private sector, civil society organisations, the technical community and the academia.

For further information, Research ICT Africa can be contacted via: info@researchictafrica.net or at +27 21 447 6332.

Introduction

The current debate and approach to protect internet users from cyber-attacks revolve around the establishment of cyber-threats. The main risk of such an approach is that it may create a pervasive sense of vulnerability among the citizenry as it comes with a heightened sense of anxiety, urgency and insecurity to access and use the internet. Even worse, the chilling effect[1] resulting from a climate of militarisation and securitisation of the internet may put on hold a positive trend of increasing internet access and use which is necessary for the socio-economic development of the country.

Currently, the only empirical evidence on cyber-threats is provided by commercial organisations involved in internet and computer-related security which may have a commercial interest in creating alarmism among the citizenry. Despite the increasing attention cyber security is getting in security politics, it seems that cyber incidents are causing minor and occasionally major inconveniences.

Research ICT Africa is concerned that potential cyber-threats identified by Governments aligned with the US War on Terrorism, have become the main reason why the South African government is imposing draconian restrictions and regulations on the internet although the current status of cyber-threats and cyber-crime has not been properly measured and assessed. Cyber-threat representations must be well documented and penalties well balanced with the crime at all times in order to rule out (over)reactions with too high implementation costs and uncertain benefits. Unintended consequences of such an approach are already visible with the disproportionate penalty faced by MTN Nigeria for failing to register over 5 millions SIM cards active on its network, despite very little evidence of SIM card registration effectiveness to safeguard digital security and physical safety.

The current approach to fighting cybercrime enshrined in the Draft Bill is characterized by state-centrism, top-down hierarchical control and erection of preventive legislative perimeters to eliminate potential cyber-threats. This approach is contrary to the multi-stakeholder, bottom-up, horizontal, and un-regulated setting which has allowed the Internet grow and expand. RIA is cognizant of the cyber-threats citizens, public and private organisations, are exposed on the internet and therefore it well receives the commitment of the South African government to address these risks from a public interest point of view. Nevertheless, the approach adopted in the Draft Bill undermines certain constitutional rights which South African citizens are expected to enjoy offline and online. Therefore, **we recommend the Department of Justice to withdraw the Draft Bill in its entirety.**

In the remainder of the submission, the main concerns with the Draft Bill are identified, and we highlight significant problems related to potential infringement of constitutional rights of freedom of expression, access to information, and privacy.

[1] In a legal context, a chilling effect is the inhibition or discouragement of the legitimate exercise of natural and legal rights by the threat of legal sanction. The right that is most often described as being suppressed by a chilling effect is the constitutional right to free speech.

Broad, overarching and potentially open to abuse list of cyber-crimes

Currently, in South Africa most online crime is governed by the Electronic Communications and Transactions Act (ECTA) of 2002, Chapter XIII.

The Draft Bill seeks to initiate a long list of new cybercrime offences with harsh penalties for unlawful access to, or interference with, private data; distributing malware, phishing attacks along with other offences. It also deals with issues related to internet content as it places harsh penalties on the distribution of data messages that promote hate, discrimination and violence (Section 4-Section 22).

The list of cybercrime offences is broad and overarching and expands on the original sections of the ECTA.

The main problem with such a broad list of cyber-crimes is that it could result in the criminalisation of cybersecurity and digital safety professionals, such as security analysts and researchers who try to detect and block malicious behaviour in network traffic and identify cyber-risks as part of their civil and academic duties. These tests are run in order to identify and fix security flaws that may put internet users at risk. Nevertheless, according to the list of cyber-crime offences envisaged in the Draft Bill, cybersecurity and digital safety professionals may be considered guilty of conducting such tests, until proven innocent.

Chilling effect on the constitutional right to free speech

The Draft Bill's prohibitions on the dissemination of hateful and violence inciting material are plausible. Nevertheless, its definition of hate speech seems broader than the one contained in the Constitution. On the one hand, it does not envisage a harm test and extends the grounds for hate speech beyond race, gender, ethnicity or religion; on the other hand its definitions of harmful and content inciting violence go farther than the constitutional exception to freedom of expression to deal with hate and violent speech.

Clause 17 of the Bill criminalizes the "*dissemination of [a] data message which advocates, promotes or incites hate, discrimination or violence*". At first sight, clause 17 provides that, "*Any person who unlawfully and intentionally–(a) makes available, broadcasts or distributes; (b) causes to be made available, broadcast or distributed; or (c) assists in making available, broadcasts or distributes […] to a specific person or the general public, a data message which advocates, promotes or incites hate, discrimination or violence against a person or a group of persons, is guilty of an offence.*" While it appears innocuous, even laudable, since it seems to emulate Section 16(2) of the Constitution (i.e. omissions to freedom of expression), it should be received with caution and scrutinised for further unintended consequences. Unintended consequences of this section are related to making unlawful the distribution, sharing or broadcasting of prohibited speech, even for the purposes of analysis, comment or public discourse, which may lead to chilling effect. Not only is the term "unlawful" vague and open to interpretation. For instance, it would constitute a criminal offense to share a link to an article or video which may be considered prohibited speech by a public authority. Such an arrangement, potentially unconstitutional, may constitute an unreasonable restriction on freedom of information.

The prohibition of incitement to violence is also overbroad. The constitutional test requires the threat of violence to be imminent (Chapter 2: SA Bill of Rights, Art. 16.2). The risk of overbroad provisions could well lead to constitutionally indefensible censorship of internet content.

Electronic communications service providers (ECSP) to police the Internet

Chapter 1, Section 1 "Definition and interpretation" provides a far reaching definition of electronic communications service provider (ECSP), including not only entities providing an electronic communications service under and in accordance with an electronic communications service licence issued under Chapter 4 of the 2005 Electronic Communication Act, but also financial institutions and any "*person or entity who or which transmits, receives, processes or stores data",* which seems to include anybody dealing with someone else data.

The unintended and problematic consequences of such a far-reaching definition are evident considering the pressure and extensive obligations imposed on ECSPs. Under section 64 of the Draft Bill, ECSPs will be required to report any criminal activity on their networks which may include also legitimate acts including file-sharing. Specifically, clause 64 (i.e. General obligations of electronic communications service providers and liability) of the Bill provides that an ECSP must:

> *(a) Take reasonable steps to inform its clients of cybercrime trends which affect or may affect them;*
>
> *(b) Establish procedures for its clients to report cybercrimes with the electronic communications service provider; and*
>
> *(c) inform its clients of measures which can be taken in order to safeguard itself against cybercrimes [if it becomes aware that its computer network or electronic communications network is being used to commit a cybercrime].*
>
> *(d) Immediately report to the National Cybercrime Centre; and*
>
> *(e) Preserve any information which may be of assistance to the law enforcement agencies in investigating the offence.*

An ECSP's failure to comply constitutes an offence, which is punishable with a fine of ZAR10,000 for each day of non-compliance.

As currently defined by the Draft Bill, many of the ECSPs do not have either the economic or technical capacity to implement the obligations entrusted to them.

Risk of surveillance on citizens' privacy

In addition to the impossibility of the majority of ECSPs complying with the obligations entrusted to them, clause 40 (Expedited preservation of data direction) specifies that ECSPs need to maintain their clients' data even when the Regulation on Interception of Communications and Provision of Communications Related Information Act (RICA) does not require an entity to intercept, record, or store information.

In this way, the Draft Bill seems to create a parallel procedure to the much contested RICA for the investigation, search and seizure of electronic communications and data. This seems to provide wider surveillance powers with fewer checks and balances than RICA.

The Draft Bill's grounds for the issuing of a search warrant are even more than RICA's already opaque grounds for the issuing of interception directions. An investigator in such cases does not even have to be a law enforcement officer: he or she can merely be an

"*appropriately qualified, fit and proper person*", although operating under the supervision of a law enforcement officer and appointed by the National Commissioner or the Director-General: State Security.

Similar to RICA, the Draft Bill does not make provision for the users to be notified after a warrant has been issued, in violation of their rights to communicate privately and to employ legal protection.

It is important to emphasize that forms of surveillance by public institutions may violate individuals' right to privacy if pursued without court approval by a law enforcement officer and without a warrant notification.

In addition to that, the Draft Bill grants a concerning level of discretion to a State's security cluster. The Draft Bill creates a host of new state institutions, falling under the Minister of State Security and the Minister of Defence, to counter cybercrime and cyberterrorism.

Specifically, the Draft Bill creates a Cyber Response Committee made up of about 13 people. The chairperson will be the Director-General: State Security. The Minister of State Security is expected to establish and operate:

- a Cyber Security Centre and appoint someone from the State Security Agency as its Director, and
- one or more Government Security Incident Response Teams and appoint someone from the State Security Agency as the head of each one.

The Minister of Defence must establish and operate a Cyber Command and appoint someone as the General Officer Commanding.

The coordination of these institutions by the Cyber Response Committee chaired by the Director-General: State Security place them under the political control of the state security ministry, undermining the principle of regulatory independence required to efficiently regulate the internet.

Risks of militarisation of the internet are evident in the far-reaching powers granted to the South African Police Service and the State Security Agency to investigate, search, access and seize just about anything, with verbally granted search warrants being deemed sufficient for them to take action they deem appropriate (Section 30, Oral application for search warrant or amendment of warrant).

In this way, the Cybercrimes and Cybersecurity Bill gives the South African Police Service and the State Security Agency (and their members and investigators) extensive powers to investigate, search, access and seize any electronic device including databases or networks wherever it might be located even without a search warrant (Section 31, Search and access or seizure without search warrant).

State security is not the most appropriate institution to be tasked with this responsibility. It leans towards secrecy and therefore its existing activities may lack democratic controls. It operates with an overly broad mandate. Yet in spite of these systemic weaknesses, if the Draft Bill is passed in its current form the State Security Agency will be given additional responsibilities, including the power to interfere unduly in internet governance issues including internet content and privacy.

Unconstitutional ban on access to public-sector information

Section 5 of the Draft Bill describes unlawful interception of data. It classifies the interception of data as:

> *"The acquisition, viewing, capturing or copying of data through the use of a hardware or software tool contemplated in section 6(5) or any other means, so as to make some or all of the data available to a person other than the lawful owner or holder of the data, the sender or the recipient or the intended recipient of that data".*

In addition to the fact that the term "unlawful" is vague and open to interpretation, the list of sources mentioned in section 5 includes National Critical Information Infrastructures (NCII). The definitions provided by the Draft Bill of critical data and "national critical information infrastructure" are overbroad; those include

> *"any data storage medium, computer device, database, computer network, electronic communications network, electronic communications infrastructure or any part thereof or any building, structure, facility, system or equipment associated therewith or part or portion thereof or incidental thereto-*
>
> *[…]*
>
> *(b) which, for purposes of Chapters 2 and 4 of this Act, are in possession of or under the control of*
>
> > *[…]*
> >
> > *(i) any department of State or administration in the national, provincial or local sphere of government;*

This means that "*any data storage medium, computer device, database, computer network, electronic communications network, electronic communications infrastructure or any part thereof or any building, structure, facility, system or equipment associated therewith or part or portion thereof*" owned by a public institution is declared critical. The danger of such broad definition is that it may reduce transparency and intensify secrecy as it limits access to data and information produced, stored, and owned by the public sector.

Such a broad definition is in contrast even with international guidelines provided by the International Telecommunications Union which defines critical infrastructure narrowly, as being what is so vital to a country that its incapacity or destruction would have a catastrophic impact.

The Draft Bill criminalises unlawful interception of, and access to, online information, and prescribes particularly harsh penalties for computer-related espionage. Clause 16(5)(b) of the Bill provides that

> *"Any person who unlawfully and intentionally–(i) possesses; (ii) communicates, delivers or makes available; or (iii) receives, data which is in the possession of the State and which is classified as confidential [by the State], is guilty of an offence."*

Clause 16(5)(b) mirrors the controversial Protection of State Information Bill (POSIB)[2] which criminalises reporting on classified state information and intentionally accessing leaked information. The approach to computer-related espionage and unlawful access to restricted data envisioned in the Draft Bill entrenches some of the most worrying features of POSIB in the sense that it restricts the constitutional right to access to public-sector information. Therefore, according to the Draft Bill, those reporting on matters of public interest could potentially be criminally prosecuted, even if they act according to a constitutional right to access to public information.

Section 32 of the Constitution of South Africa protects *"the right of access to any information held by the state; and any information that is held by another person and that is required for the exercise or protection of any rights."* This right is implemented through the Promotion of Access to Information Act of 2000.

Final remarks

The Draft Bill threatens our constitutional rights in significant ways, specifically those relating to freedoms of expression and of information, the right to privacy, and the right to access to public-sector information. It lacks important checks and balances and unnecessarily heightens state power over the internet in many ways.

The South African Government's race to secure and militarise the internet in the name of protecting South African citizens from potential cyber-threats enables to Government's control of the internet and surveillance of its citizens.

Taking into account the long list of cyber-crimes provided by in the Draft Bill, law enforcement agencies will be overwhelmed with cybercrime cases and understaffed to tackle the cyber-threats envisaged by the Draft Bill. They may lack the necessary capacity and competencies to assess case-by-case whether an action is legitimately considered cyber-crime and subsequently respond to it.

In addition to the potential inability of the public sector to tackle hypothetical attacks in the most effective way, we are particularly concerned with the risk arising from the potential abuse of power endorsed under Section 31 of the Draft Bill to law enforcement agencies or investigators who are granted the ability to search and access or seizure of evidence without search warrant where cybercrimes are suspected. This may place legitimate online activities at risk of criminalisation at discretion of public officials.

The efficiency of the Internet, on a technical level, is founded on open and distributed networks of local engineers who share information as peers in a community of practice rooted in the university system. The internet functions because of the absence of centralised control. These decentralised mechanisms already in place can form the basis of a coherent distributed security strategy. A distributed security strategy should enable ways to facilitate cooperation among existing and largely scattered security networks while making their actions more transparent and accountable.

The Draft Bill seems to focusing on securing the Internet by heightening state powers to act arbitrarily and unaccountably rather than safeguarding citizens' right. It seems to

[2] The Protection of State Information Bill (POSIB) aims to implement a system to regulate state information, but instead places harsh restrictions on the possession or distribution of classified state information with penalties of up to 25 years in prison. Individuals who intentionally access leaked information, including internet users, would be held criminally liable and face up to 10 years in prison.

characterise cyber-risks as an existential threat in an attempt to justify extraordinary measures such as the suspension of civil and political liberties. Research ICT Africa is supportive of the creation of a safe and trusted Internet and believes that many online problems (such as phishing and malware) could be dealt with through collaborative efforts between the state, industry, the technical community, and society. To this it offers unconditional support. It does not believe this proposed law creates such a collaborative, transparent and accountable framework. Rather it appears to legitimise greater censorship, militarisation, and surveillance of the State online. For these reasons, we propose the Department of Justice to withdraw the Cybercrime and Cybersecurity Bill in it entirety.

References

Deibert, R., and Rohozinski, R. (2009). Tracking ghostnet: Tracking a cyber-espionage network. Toronto: Information Warfare Monitor, University of Toronto. The Centre for International Governance Innovation. Internet Governance Papers. Paper No. 6 – October 2013.

Deibert, R. J. (2013). Bounding Cyber Power: Escalation and Restraint in Global Cyberspace.

Dunn Cavelty, M. (2012). The Militarisation of Cyberspace: Why Less May Be Better. 2012 4th International Conference on Cyber Conflict.

Hjalmarsson, O. [2013]. The Securitization of Cyberspace. How the Web Was Won. Lund University. Department of Policy Science. STVK02.

Gillwald, A. (2015). African nations use SIM card question to mandate control. In BusinessDay, Opnion & Analysis. Available at http://www.bdlive.co.za/opinion/2015/11/26/african-nations-use-sim-card-question-to-mandate-control