Internet Service Providers' Association

queries@ispa.org.za
010 500 1200
http://www.ispa.org.za
PO Box 518, Noordwyk, 1687

30 November 2015

The Department of Justice and Constitutional Development

Attention: Mr. SJ Robbertse

Per e-mail: cybercrimesbill@justice.gov.za

Dear Sir

DRAFT CYBERCRIMES AND CYBERSECURITY BILL 2015

1. Introduction

1.1. The Internet Service Providers' Association (ISPA) refers to the draft Cybercrimes and Cybersecurity Bill ("**the Draft Bill**") and the accompanying Discussion Document as published for comment by the Department of Justice and Constitutional Development ("**the Department**").

1.2. ISPA takes note of

1.2.1. The increase in broadband penetration and access to the Internet in South Africa which – paired with low digital literacy rates and law enforcement capacity constraints – creates an environment in which cybercrime is increasing.

1.2.2. The Justice Crime Prevention and Security Cluster (JCPS) Outcome 3 deliverables with specific reference to Output 7: Secure cyber space and the implementation strategy set out in the Refined Delivery Agreement for Outcome Three: All People in South Africa Are and Feel Safe.

1.2.3. The need to ratify the Budapest Convention.

1.2.4. The experience of our own members in interacting with law enforcement authorities and the need for greater certainty in the framework governing such interaction.

1.2.5. The general requirement to implement measures for a more coherent approach to dealing with cybercrime.

1.3. ISPA therefore welcomes the publication of the Draft Bill, and looks forward to constructive, evidence based interaction with the Department in ensuring that the final legislation is fit for purpose.

1.4. We are keenly aware of the complexity of drafting legislation of this nature as well as the imperative on the drafters to be as inclusive as possible so as to ensure that law enforcement has all the required tools at its disposal. We therefore:

1.4.1. Commend the Department for the extended public participation process which it is engaging in.

1.4.2. Request that the submissions below are accepted in the constructive light with which they are intended.

1.4.3. Request the opportunity to workshop relevant clauses with the Department and law enforcement representatives.

_____

2. ISPA's interest in the Draft Bill

2.1. ISPA is a South African Internet industry body not for gain. ISPA is a voluntary organisation, representing the interests of its members.

2.2. Established on 6 June 1996, ISPA currently represents in excess of 150 Internet Service Providers with a range of services and target markets. ISPA's membership comprises a blend of providers of network and communications services, as well as resellers of network and communication services.

2.3. The Minister of Communications formally recognised ISPA as an Industry Representative Body in terms of section 71 of the Electronic Communications and Transactions Act, 2002 on 20 May 2009.

2.4. The majority of ISPA's members fall squarely under the definition of 'electronic communication service provider – "ECSP".

2.5. ISPA has also proactively engaged with law enforcement authorities and other stakeholders to:

2.5.1. Develop a shared understanding of the legal framework applicable to the interaction between law enforcement and ISPA members.

2.5.2. Facilitate co-operation between ISPA members and law enforcement authorities within such framework.

2.5.3. Train law enforcement agencies in Internet-related issues.

2.5.4. Provide information to and assist consumers with cybercrime issues.

2.5.5. Develop the icode[1] project, which is an industry-driven initiative to identify infected machines, inform affected consumers that they may be at risk, provide support to enable those consumers to disinfect their machines, and reduce their risk of re-infection.

2.5.6. Develop shared resources such as posters to assist with consumer awareness around cybersecurity issues[2].

2.6. As such ISPA has - and its members have - a direct interest in the Draft Bill.

---

[1] www.icode.org.za, see further below.

[2] http://ispa.org.za/social-development/poster-project/ and see examples provided in Annexure A.

3. Scope of submissions

3.1. ISPA will address only those provisions of the Draft Bill that fall within the main concerns of its membership:

3.1.1. Chapter 1 – Definitions;

3.1.2. Chapter 6 – Structures to deal with cybersecurity;

3.1.3. Chapter 7 – National Critical Information Infrastructure Protection; and

3.1.4. Chapter 9 – General obligations of Electronic Communications Service Providers read with Chapter 4.

3.2. In order to put these submissions into perspective, ISPA first makes some general submissions in regards to the following:

3.2.1. Offline world vs the online world;

3.2.2. Analysis of public IP blocks and autonomous system numbers allocated or assigned by AFRINIC;

3.2.3. ISPA and its members' existing obligations;

3.2.4. Existing ISPA initiatives; and

3.2.5. Neutrality of ISPA's members as intermediaries

_____

4. General submissions

4.1. Offline world vs the online world

4.1.1. ISPA has a fundamental concern with the general trend in various on-going legislative initiatives that its members are treated differently to their analogous counterparts in the offline world.

4.1.2. This flows from the following statement in paragraph 3.9 of the Discussion Document:

Due to the mechanics of the Internet, the transmission of a communication involves a number of entities. For instance, in order to download child pornography, the content provider who uploaded the material (for example on a web storage facility), the access provider who provides access to the Internet, the hosting provider who provides the storage facility, the access provider who provides a person with access to the web storage facility halfway across the globe, are involved. Because of this involvement electronic communications service providers are always part of the investigation of criminal offences and law enforcement agencies are dependent on the cooperation of electronic communications service providers. Electronic communications service providers cannot monitor communications unless they are authorised to do so under judicial authority. On the other hand electronic communications service providers operate in a highly regulated environment which imposes obligations on them regarding the way in which they conduct their daily business, which are aimed at protecting their customers in cyberspace. For purposes of the Bill, electronic communications service providers are defined broadly so as to encompass other persons and entities, which are not traditionally regarded as electronic communications service providers.

4.1.3. In order to illustrate this concern, we refer to the fictitious offline example set out below.

Example: Armed robbery

The 23'ers – a gang based in Midrand – decides to rob a cash in transit vehicle at the casino close to OR Tambo International Airport. In the execution of their crime, they have to:

a) Travel by car to the Gautrain station
b) Travel to OR Tambo by train
c) Travel to the casino by taxi (booked through Uber)
d) Hold the security guards up on the premises of the casino
e) Travel back to their car using taxi and train as mode of transport

f) Get in their car, cross municipal, provincial roads and national road infrastructure to arrive at their destination where they will distribute the proceeds of their crime amongst themselves.

Critical to the success of their operation is the need to be in constant communication with each other by means of cellular phones.

4.1.4. In this example – compared to for example the appropriation of data - we can draw the following direct comparisons to the online world:

Offline – cash in transit heist	**Online – appropriation of data**	**Online service provider**
Cash	Data	
Security Guards	Firewall and passwords	Electronic security services provider
Casino premises	Data Centre	Data centre providers
Cash in transit truck	Computer server	Owner of server infrastructure
Railway Roads	Access, metro area and national electronic communications networks	Electronic Communications Network Provider
Gatekeeper at the train station	Internet Service Provider	Electronic communications service provider
Uber	Over-the-Top service provider	Applications developers
Weapons	Malware	Providers of malware
Telephone communication	Telephone communication	Electronic communications service providers

4.1.5. The complexities involved in the prevention, investigation and prosecution of any illegal activity are the same, regardless of the realm that it occurs in. Consequently, the line of argument in paragraph 3.9 at page 76 of the Discussion Document (quoted above) holds as much weight in the offline world as it does in the online world.

4.1.6. Given that the example would not be classified as "cybercrime", why would there be different obligations and sanctions applicable to the cell phone operators for assisting law enforcement agencies with providing relevant evidence, compared to having to provide the same information in relation to an offence set out in the Cybercrime Bill?

4.1.7. By extension, why would there have to be a differentiation with any other provider of electronic communication services?

4.1.8. Would it make sense to create obligations and criminal sanctions similar to those in the Cybercrime Bill for the motor vehicle manufacturer, Gautrain, the roads agencies, Uber, taxi drivers, security guards and vehicle fleet owners as suppliers of products and services that was involved in the example?

4.1.9. ISPA thus poses the question: why then should its members and related industry players be dealt with differently to offline suppliers of products and services?

4.2. Analysis of public IP blocks and autonomous system numbers allocated or assigned by AFRINIC

Autonomous Systems Numbers

4.2.1. Within the Internet, an autonomous system (**AS**) is a collection of connected Internet Protocol (IP) routing prefixes under the control of one or more network operators on behalf of a single administrative entity or domain that presents a common, clearly defined routing policy to the Internet. Each ISP[3] must have an officially registered autonomous system number (**ASN**) in order for its network to be connected to the Internet.[4]

4.2.2. Organisations that do not offer electronic communications services to the public can also have their own private network connected to the Internet if its network has its own ASN.

4.2.3. It therefore follows that any data that traverses the Internet can only pass through networks with an ASN.

4.2.4. Having done some basis desktop analysis on assigned ASNs to South African entities, ISPA notes that there is a substantial amount of organisations other than electronic communications services providers that have ASNs assigned to it, as illustrated in Chart 1 below.

[3] The term "ISP" is used to describe an entity which would generally be regarded as one which provides access to the Internet on a commercial basis.
[4] RFC 1930, Section 3

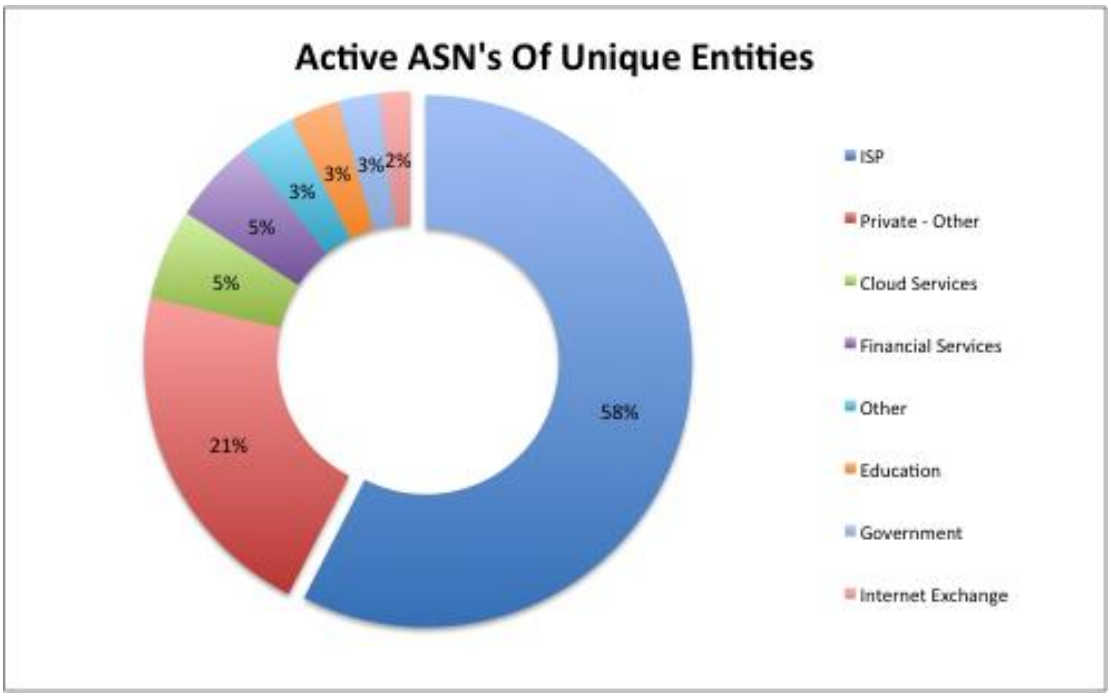

Chart 1 – Estimated distribution of ASNs

4.2.5. In addition to the distribution of assigned ASNs, the ratio of electronic services providers with ASNs compared to the total amount of service providers is also quite important to take note of. Chart 2 below illustrates this ratio.

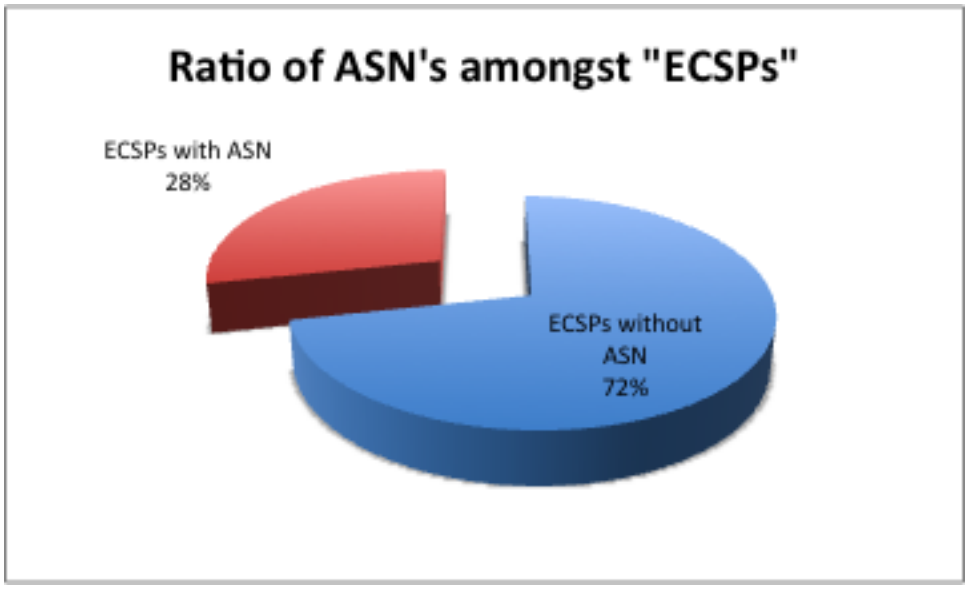

Chart 2 - Estimated ratio of ECSPs with ASNs to ECSPs without ASNs

4.2.6. Chart 2, viewed collectively with Chart 1, illustrates the following:

- The vast majority of ECSPs are resellers of a much smaller group of upstream providers;
- The smaller group of upstream providers comprise only a portion of types of entities that would have the infrastructure and systems in placed as is assumed to be in the exclusive domain of ECSPs.
- Private institutions, government and universities "own" almost as many autonomous networks as those owned by ECSPs.

Public IP blocks

4.2.7. An Internet Protocol address (**IP address**) is a numerical label assigned to each device (e.g., computer, printer) participating in a computer network that uses the Internet Protocol for communication.[5] An IP address serves two principal functions: host or network interface identification and location addressing.

4.2.8. IP addresses are allocated or assigned to South African organisations in "blocks" by AFRINIC. Those entities to whom IP address have been allocated / assigned are thus the relevant entities who manage and control to whom or what the individual IP addresses assigned / allocated to them are issued.

4.2.9. Since no device can connect to the Internet without an IP address, it follows that it would be most beneficial to understand to whom public IP address have been allocated / assigned.

[5] RFC 760, DOD Standard Internet Protocol

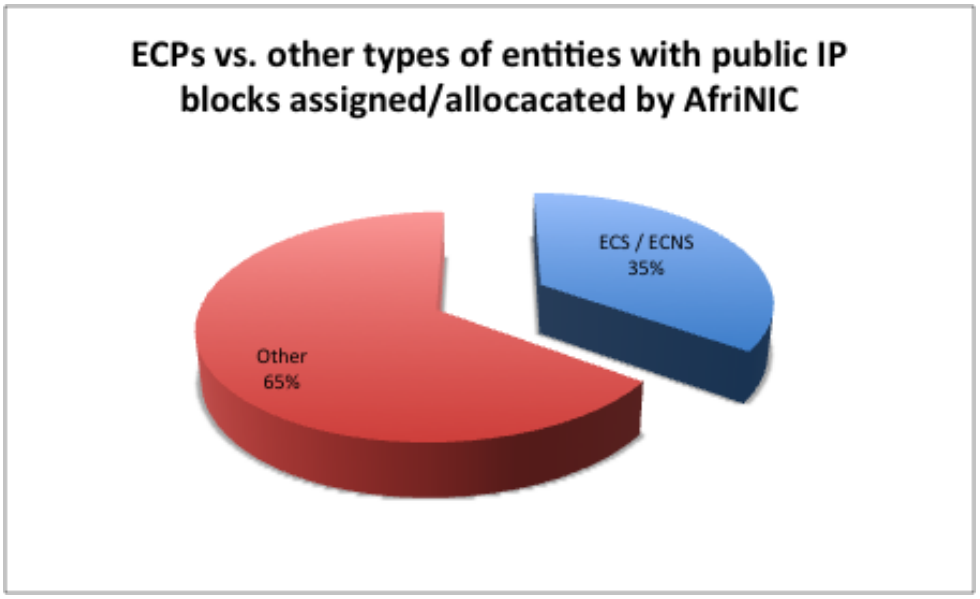

Chart 3 - Estimated ratio of ECSPs with public IPs

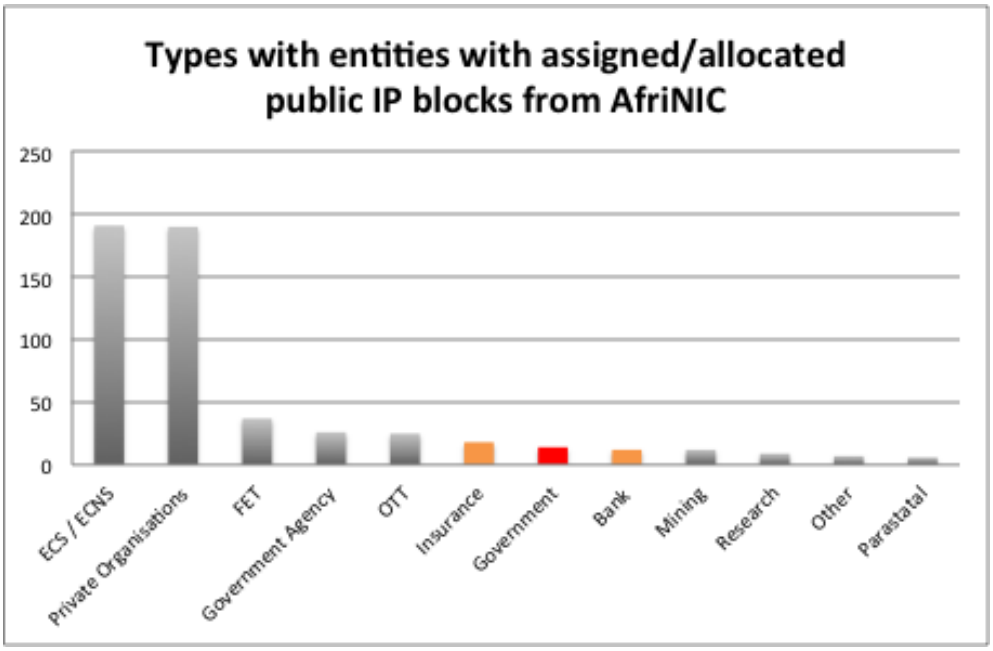

Chart 4 - Estimated distribution of entities with public IPs

4.2.10. From chart 3 and chart 4 it becomes evident that:

- The ratio of unique ECSPs with public IP address is approximately only one third of the entities that have public IPs allocated / assigned to them.
- The range of entities that are in possess of its own block(s) of public IPs is a diverse mix of private and public entities involved in a multitude of industries.

4.2.11. Given the above explanation of ASNs and IP addresses, with its brief and high level overview, ISPA submits that it is quite possible that anybody from a university to a vehicle manufacturing company could "own" its own IP address blocks distributed across its own autonomous system number. Such an entity would be able to furnish more information to a law enforcement agency than the vast majority of ECSPs would be able to do. Should such entities be regarded as falling within the definition of ECSP?

4.2.12. ISPA submits that no court would extend the definition of ECSP to such entities. If it is the intention that such persons be deemed to be ECSPs, then the public participation process would probably have some shortcomings in that it could not reasonable be expected of (for example Anglo American) to expect that it has a vested interest in having to participate in draft criminal legislation.

4.2.13. More relevant to the ISPA membership, the analysis serves to illustrate that the line of argument in paragraph 3.9 at page 76 of the Discussion Document seems to be premised on a misunderstanding of the Internet industry. Whilst it is correct that data traversing the Internet requires a concatenated web of various suppliers of services, the reality is that the systems and body of knowledge required of ECSPs in the Draft Bill are located in a very limited number of suppliers.

4.2.14. As such, ISPA submits that some further thought needs to be applied to ensure that the relevant and correct class of entities that would be of assistance in the prevention and investigation of cybercrimes are identified.

4.3. ISPA and its members' obligations

4.3.1. As stated above, ISPA is an Industry Representative Body recognised by the Minister of Communications in terms of section 71 of the Electronic Communications and Transactions Act.

4.3.2. This recognition was provided to ISPA pursuant to the *Guidelines for Recognition of Industry Representative Bodies of Information System Service Providers*[6] *(*the **"IRB Guidelines"**).

4.3.3. Relevant to this submission, the IRB Guidelines were drafted to, amongst other things:

- Increase the legality, integrity and safety of the Internet[7]
- Ensure respect for fundamental rights and freedoms and principles governing public order and safety[8]
- Promote confidence in the use of the internet[9]

4.3.4. In respect of cybercrime, the IRB Guidelines deal with the following:

[6] Gazetted under GN 1283 in GG 29474 of 14 December 2006
[7] IRB Guidelines, regulation 3.7
[8] IRB Guidelines regulation 3.9
[9] IRB Guidelines, regulation 3.10

- ECSPs (or ISPs as used in the guidelines) must commit to assisting law enforcement agencies in legitimate investigations[10]
- Members must implement all reasonable measures to prevent the unauthorised access to, interception or interference with data under its control[11]
- Various measures pertaining to[12]
    - Prevention
    - Education
    - Identification and preservation
    - Reporting
    - Establishing a point of contact

4.3.5. The minimum standards expected of ISPA and its membership has also been incorporated into the ISPA Code of Conduct in paragraphs F through to I[13]:

F. Cyber crime

16. ISPA members must take all reasonable measures to prevent unauthorised access to, interception of, or interference with any data on that member's network and under its control.

G. Protection of minors

17. ISPA members must take reasonable steps to ensure that they do not offer paid content subscription services to minors without written permission from a parent or guardian.
18. ISPA members must provide Internet access customers with information about procedures and software applications which can be used to assist in the control and monitoring of minors' access to Internet content. This requirement does not apply to corporate customers where no minors have Internet access.

H. Lawful conduct

19. ISPA members must conduct themselves lawfully at all times and must co-operate with law enforcement authorities where there is a legal obligation to do so.
20. ISPA members must respect intellectual property rights and not knowingly infringe such rights.

[10] IRB Guidelines, regulation 3.7
[11] IRB Guidelines, regulation 2.8
[12] IRB Guidelines, regulation 6
[13] available at http://ispa.org.za/code-of-conduct/.

21. ISPA members must uphold and abide by this Code of Conduct and adhere to the associated complaints and disciplinary procedures.

I. Unlawful content and activity

22. There is no general obligation on any ISPA member to monitor services provided to customers, but a member is obliged to take appropriate action where it becomes aware of any unlawful content or conduct.

23. ISPA members must not knowingly host or provide links to unlawful content, except when required to do so by law.

24. If an ISPA member becomes aware of conduct or content which has been determined to be illegal, it must suspend or terminate the relevant customer's service and report the conduct or content to the relevant law enforcement authority. The ISPA member must report such cases and any action taken to ISPA within a reasonable period of time.

25. ISPA members must establish a notification and take-down procedure for unlawful content and activity in accordance with ISPA's take-down notification procedure, and respond expeditiously to such notifications.

26. ISPA members must submit a report to ISPA on the steps taken in response to a take-down notice within a reasonable period of time after such a notice is lodged.

27. ISPA members must keep a record of all take-down notices received and any materials taken down for a period of at least three years unless possession of such materials is illegal.

4.3.6. ISPA submits that the Department should have regard to the principles set out in the IRB Guidelines insofar as these apply to ECSPs/ISPs and that requirements should be fair and not adversely affect the economic viability of ECSPs/ISPs.

4.3.7. In particular, the IRB Guidelines provide that the minimum standards set out therein are regarded as sufficient to achieve the goals set out in the IRB Guidelines. ISPA submits that the Cybercrime Bill should not impose stricter standards on ISPA's membership than those already provided for in the IRB Guidelines.

4.4. Existing ISPA initiatives

4.4.1. In addition to and in furtherance of the IRB Guidelines and ISPA Code of Conduct, ISPA has also initiated the icode project. This project aims to educate and assist consumers with cybercrime and related issues, with particular reference to the large number of consumer devices that have been compromised by criminals and infected with malware, spyware and viruses. These machines are commonly referred to as "zombies" and networks of zombie machines are called "botnets". So-called zombie botnets are used for criminal activities including identity theft, distribution of child pornography, facilitation of phishing attacks and other illegal activities.

4.4.2. The icode is in part a response to the prevalence of infected machines in South Africa and the likelihood that this will be aggravated by large numbers of new users coming online with low levels of digital literacy.

4.4.3. Participants in the icode may seek to identify infected machines, inform affected consumers that they may be at risk, provide support to enable those consumers to disinfect their machines, and reduce their risk of re-infection.

4.4.4. The objectives of the icode are:

4.4.5. The objectives of the icode are:

- to instil a culture of cyber security within South African ISPs and their customers;
- to provide a consistent message in plain language to customers, in order to raise awareness of cyber security risks, educate users on steps that they can take to better protect themselves online, and to assist customers who may have infected machines;
- to encourage ISPs to identify compromised computers on their networks;
- to develop mechanisms for ISPs to share information and collaborate on cyber security concerns affecting South Africa ISPs; and
- to encourage ISPs to identify and report any cyber security issues that may affect South Africa's critical infrastructure or that may have a national security dimension

4.4.6. Participation is not limited to ISPA members.

4.4.7. More information can be obtained from http://icode.org.za.

4.5. Neutrality of ISPA's members as intermediaries

ECSPs are not organs of state involved in the investigation of crime. There must be clarity on the reporting requirements of ECSPs and the circumstances under which it can be said that they are aware of the use of their services for the commission of a crime. In particular, it is of critical importance to ISPA that the neutrality of its members acting as "mere conduits" is recognised and upheld throughout the provisions of the Draft Bill.

5. Submission on specific Focus Areas

5.1. Chapter 1 – Definitions

5.1.1. Definitions within definitions

ISPA notes that there are various defined terms within definitions that lead to absurd interpretations.

In particular, the term "electronic communications network" is included in the definition of "computer device", "computer network" and "National Critical Information Infrastructure". All three last mentioned terms exist throughout the Draft Bill as distinctly separate concepts from an "electronic communications network".

ISPA submits that this should be considered and rectified.

5.1.2. Definition of electronic communications network

ISPA submits that the definition for an "electronic communications network" is vague and confusing, and that reference should be made to the definition of an electronic communications network as set out in the Electronic Communications Act, 36 of 2005 (the **"ECA"**).

Having regard to the various crimes set out in the Draft Bill, it may be required to distinguish between the internet (being a network of interconnected networks), Wide Area Networks, Local Area Networks (small networks) and Private Networks. All these networks are defined in the ECA or the Service Licence Exemption Regulations 2008.

5.1.3. Definition of electronic communications service provider

Having regard to the ISPA submissions in paragraph 4.2 above, ISPA submits that the definition of ECSP is far too wide, is vague and leads to absurdity.

In particular, ISPA submits that:

- Financial institutions should not be included in definition of ECSP. Financial institutions and those provisions in the Draft Bill that applies to financial institutions as opposed to ISPs should be clearly identifiable and distinguishable.
- Persons referred to in subsection (c)(i) are already covered under subsection (a) to the extent that the latter covers resellers and the definition of "electronic communications service provider" is intended to match the obligations to be imposed on them.

- Subsection (c)(ii), ECSP includes any person who transmits, receives, processes or stores the data of "any other person". We submit that this is overly broad and strains the general understanding of what an ECSP is and what it does.

In addition to the exclusions submitted above, ISPA notes that the definition of ECSP does not include electronic communications network service providers as defined in the ECA. ISPA submits that these licensees are a class of licensees that are often just as well or even better equipped to perform the functions envisaged in the Draft Bill.

However, as illustrated in paragraph 4.2 above, not all ECNS and ECS licensees would have the systems or skills to fully comply with the expectations underlying the various obligations set out for ECSPs in the Draft Bill.

ISPA submits that a fresh approach is required that identifies the correct classes of entities within the Internet value chain, in order that expectations pertaining to roles, obligations and other requirements can be appropriately matched to such classes of entities.

For example, in dealing with online safety, Ofcom presented a report to the House of Commons[14] that included a very simple diagram that illustrated the various stakeholders in the value chain together with the high level activities that those stakeholders could perform to ensure better governance of content.

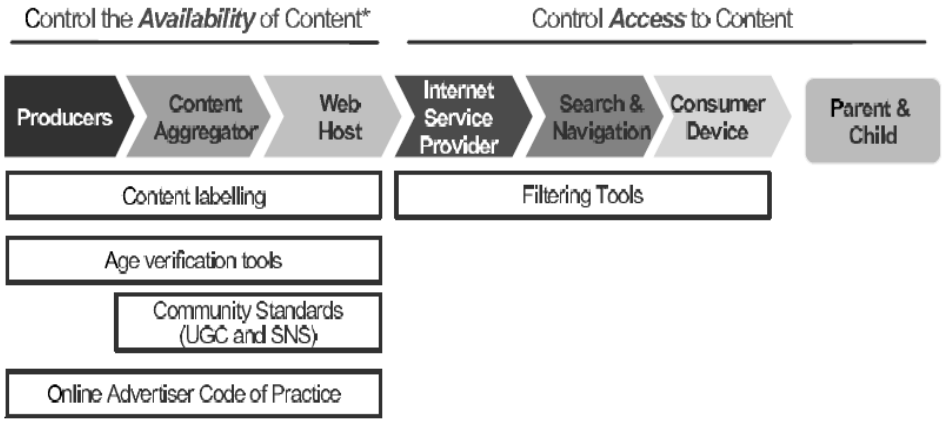

Diagram 1: Stakeholders in the online content delivery chain

Whilst Diagram 1 above may not be entirely relevant to matters pertaining to cybercrime, it illustrates how identification of various role players could assist in designing an environment that contrary to a "one-size-fits-all" and shotgun approach will provide for:

- relevant, practical and appropriate obligations on the correct class of entities
- clarity to all parties in the value chain
- less resistance from those impacted in the Draft Bill
- better implementation of the objects of the ultimate Act.

[14] Memorandum submitted by Ofcom to the House of Commons – Culture, Media and Sport in June 2008. http://www.publications.parliament.uk/pa/cm200708/cmselect/cmcumeds/353/8051302.htm

5.2. Chapter 6 – Structures to deal with cybersecurity

5.2.1. The issues of the wide definition of ECSP have been discussed at paragraphs 5.1.3 above. Amongst various problems created by the extremely wide definition of ECSP is the application of Chapter 6 to ECSPs.

5.2.2. ISPA assumes that the intention of Chapter 6 is to create various entities that have very specific and separate spheres of application. However, as the Discussion Document correctly notes, the reach of ECSPs are complex and wide.

5.2.3. In particular, ECSPs (as defined in the Draft Bill) will inevitably be involved in the provision of products and services to all the various spheres that cover all the different structures set out in Chapter 6 of the Draft Bill.

5.2.4. With that reality in mind, it is open for interpretation that all the structures created by Chapter 6 of the Draft Bill will in some form or another be found to apply to ECSPs as well.

5.2.5. ISPA has set out in table 1 below the various provisions that may be applicable to ECSPs:

Structure	Ministry	Relevant sections to ECSPs
Cyber Security Response Committee	**State Security**	51(6)(e) – Intelligence gathering 51(6)(g)(iii) – Minimum cybersecurity standards 51(6)(g)(iv) – Public Private Partnerships S51(6)(g)(v) – appropriate technical and operational cybersecurity standards
Cyber Security Centre		52(5)(f) - coordination and guidance regarding corporate security and policy development, governance, risk management and compliance, identity and security management, security information and event management and cyber forensics
National Cybercrime Centre	**Police**	(54)(4)(d) - provide coordination and guidance regarding corporate security and policy development, governance, risk management and compliance, identity and security management, security information and events management 54)(4)(h) - promote, establish and maintain public-private cooperation in order to fight cybercrime
Cyber Command	**Defence**	ECSPs provide Electronic Communications services to the Defence Force and to Critical Information Infrastructure.

Cybersecurity Hub	**Telecommunications and Postal Services**	Sect. 56(5)(c) – best practice guidelines Sect. 56(5)(e) – compliance with standards, procedures and policy of Cyber Security Response Committee Sect. 56(5)(g) - co-ordination of cyber security activities in the private sector Sectt. 56(5)(k) - cyber security audits, assessments and readiness exercises on request
Private Sector Security Incident Response Teams		Section 57(2)(a) - Each sector must, within six months from the date of the publication of a notice referred to in subsection (1)(*a*) at own cost establish one or more Private Sector Security Incident Response Teams for that sector Section 57(4) - A Private Sector Security Incident Response Team … must— *(a)* act as a point of contact between the sector entities in the sector for which it is established and the Cyber Security Hub; *(b)* be a contact point for that specific sector on cyber security matters; *(c)* coordinate cyber security incident response activities within that sector; *(d)* facilitate information-sharing and technology-sharing within the sector; *(e)* facilitate information-sharing and technology-exchange with other Private Sector Security Incident Response Teams established for other sectors and the Cyber Security Hub; *(f)* establish minimum security standards and best practices for the sector for which it is established in consultation with the Cyber Security Hub; *(g)* report all cyber security threats in the sector for which it is established and measures which have been implemented to address such threats to the Cyber Security Hub and Private Sector Security Incident Response Teams established for other sectors; *(h)* immediately report new cybercrime trends which come to its attention to the Cyber Security Hub, Private Sector Security Incident Response Teams established for other sectors and the National Cybercrime Centre; *(i)* provide sector entities within the sector for which it is established with best practice guidance on cyber security; and *(j)* perform any other function conferred on or assigned to it by the Cabinet member responsible for telecommunications and postal services by notice in the *Gazette*.

TABLE 1: STRUCTURES RELEVANT TO ECSPs

5.2.6. From Table 1 it is clear that there are various provisions that may be interpreted as being applicable to at least those ECSPs that provide electronic communications

infrastructure and related value added services to various state entities, and this would be problematic.

5.2.7. Using corporate governance as an example - it would become extremely difficult for ECSPs to have to implement and maintain different corporate governance guidelines in terms of King III, the Cybersecurity Centre, National Cybercrime Centre, Cyber Command, Cyber Security Hub and Private Sector Security Incident Response Teams.

5.2.8. ISPA submits that the issues raised in regard to Chapter 6 illustrate how important it is to prevent a "one-size-fits-all" approach, and reiterates its submission that stakeholders in the Internet value chain should be clearly identified and defined before evaluating the appropriateness and design of obligations.

5.3. Chapter 7 – National Critical Information Infrastructure Protection

5.3.1. ISPA notes that the definition of National Critical Information Infrastructure ("**NCII**") includes any other functionary or institution exercising a public power or performing a public function in terms of any legislation, irrespective of whether or not it is declared a National Critical Information Infrastructure as contemplated in paragraph (a) of the definition of NCII.

5.3.2. Furthermore, given the size and scope of some of the larger private electronic communications networks and service providers in South Africa, it is quite conceivable that sabotage of those providers would result in

(a) prejudice the security, the defence, law enforcement or international relations of the Republic;

(b) prejudice the health or safety of the public;

(c) cause interference with or disruption of, an essential service;

(d) causes any major economic loss;

(e) cause destabilization of the economy of the Republic; or

(f) create a public emergency situation.

5.3.3. With reference to entities exercising a public powers and public functions, the powers conferred on entities that hold licenses issued to them in terms of the provisions of the ECA are public powers exercised in the public interest and the services provided by them are service provided in the public interest. This is a position in law that was stated by Plasket AJA in Mobile Telephone Networks (Pty) Ltd v SMI Trading CC[15] at paragraph 33 as follows:

[15] [2013] 1 All SA 60 (SCA)

"I am of the view that the power conferred on MTN by section 22 is indeed a public power. It is a power that is central to the attainment of the primary object of the ECA, namely "to provide for the regulation of electronic communications in the Republic in the public interest". There can be no doubt that, even if MTN is motivated by the making of profit from providing its service, it is required by the ECA to provide that service in the public interest"

5.3.4. Similarly, there are a number of licensed ECN and ECNS providers within ISPA's membership that provides services that, if they were to be adversely effected, would fall within the classes mentioned in sections 58(2) (a) – (f) of the Draft Bill.

5.3.5. It therefore appears that the category of ECSPs that fall under paragraph (a) of the definition of ECSP in the Draft Bill will have to be deemed to be NCII.

5.3.6. Accordingly, it appears that any organisation providing licensed ECS and ECNS services are also NCII as defined in the Draft Bill (even though holders of ECNS licenses are not even included in the definition of ECSP).

5.3.7. ISPA submits that given the extent of requirements and obligations relevant to NCII in the Draft Bill, it would be of extreme concern to its membership if they were to be unclear as to whether their organisations would be regarded as NCII.

5.3.8. ISPA furthermore submits that its submissions in regard to NCII illustrates how important it is to prevent a "one-size-fits-all" approach, and re-iterates its submission that stakeholders in the Internet value chain should be clearly identified and defined.

5.4. Chapter 4 read with Chapter 9 – General obligations of Electronic Communications Service Providers

5.4.1. In addition to the general obligations set out in section 64 of the Draft Bill, there are also serious offences created under the provisions of sections 33(2), 38(2), 40(8)(1)(a), 41(11)(a), 47(4)(a) and 48(5)(a).

5.4.2. The Discussion document notes that the electronic communications sector is highly regulated. ISPA agrees with that observation and notes that its members are already subject to a host of general requirements and obligations. Some of these obligations arise out of the:

- Electronic Communications Act and its various regulations;
- Electronic Communications and Transactions Act and its various regulations – including the Industry Representative Body Guidelines;
- The Regulation of Interception of Communications and Provision of Communication-Related Information Act
- Films and Publications Act and its various regulations;
- Protection from Harassment Act

- Maintenance Act
- Consumer Protection Act
- Criminal Procedure Act
- National Credit Act
- Promotion of Administrative Justice Act
- The Promotion of Access to Information Act
- Common Law (including the law of public servitudes)

5.4.3. ISPA has illustrated in paragraph 0 and 4.5 above that there is no good reason why its members should be treated any different to its counterparts in the delivery of tangible products and services in the offline world.

5.4.4. ISPA reiterates is position that there is no justification for its members to be treated any differently just because they provide a different class of products and services to the public.

5.4.5. As such, ISPA submits that any special obligations and sanctions created in terms of the Draft Bill that (a) undermine the neutrality of its members in their role as "mere conduits" and (b) are inconsistent with the existing law and requirements, and should therefore be removed from the Draft Bill.

5.5. Amendment of the Criminal Law (Sexual Offences and Related Matters) Amendment Act, 2007

5.5.1. The Draft Bill proposes to amend the Criminal Law (Sexual Offences and Related Matters) Amendment Act, 2007 ("**SORMAA**") through the insertion of a series of definitions in a new section 16A, intended, it appears, to align that Act with the Draft Bill.

5.5.2. We note that the definition of ECSP to be inserted is not the same as that currently contained in section 1 of the Draft Bill:

> *(f)"electronic communications service provider" means any person who provides an electronic communications service under and in accordance with an electronic communications service licence issued to such person under Chapter 3 of the Electronic Communications Act, 2005 (Act No. 36 of 2005), or who is deemed to be licensed or exempted from being licensed as such in terms of the Electronic Communications Act, 2005."*

5.5.3. The draft Bill also seeks to insert a new section 20A insertion into SORMAA, and we refer specifically to subsections (6) and (7) read with subsections (4) and (5):

*"**Cybercrimes involving child pornography***

(4) Any person who unlawfully and intentionally—
(a) makes available, distributes or broadcasts;
(b) causes to be made available, broadcast or distributed;
(c) assists in making available, broadcasting or distributing,
child pornography by means of a computer network or an electronic communications network, is guilty of an offence.

(5) Any person who unlawfully and intentionally advocates, advertises, encourages or promotes—
(a) child pornography; or
(b) the sexual exploitation of children,
by means of a computer network or an electronic communications network, is guilty of an offence.

(6) Any electronic communications service provider who unlawfully and intentionally—
(a) makes available, distributes or broadcasts;
(b) causes to be made available, broadcast or distributed;
(c) assists in making available, broadcasting or distributing,
child pornography through a computer network or an electronic communications network, is guilty of an offence.

(7) Any electronic communications service provider who unlawfully and intentionally advocates, advertises, encourages or promotes child pornography or the sexual exploitation of children, is guilty of an offence.

5.5.4. We submit that subsections (6) and (7) should be deleted. There is no reason to single out ECSPs when they already fall within the definition of "person".

5.5.5. For the same reason the words "or electronic communications service provider" where they appear in subsection (9) should be deleted.

(9) Any person ~~or electronic communications service provider~~ who, having knowledge of the commission of any offence referred to in subsections (1) to (8), or having reason to suspect that such an offence has been or is being committed and unlawfully and intentionally fails to—
(a) report such knowledge or suspicion as soon as possible to a police official; or
(b) furnish, at the request of the South African Police Service, all particulars of such knowledge or suspicion,
is guilty of an offence.

5.5.6. The same deletion should be made to the proposed section 56A to be inserted into SORMAA.

5.5.7. We note that the Draft Bill does not seek to amend the Film and Publications Act 65 of 1996 ("the FPA"). Section 24B of the FPA also criminalises child pornography:

> ***24B. Prohibition, offences and penalties on possession of films, games and publications***
> *(1) Any person who-*
>
> *(a) unlawfully possesses;*
> *(b) creates, produces or in any way contributes to, or assists in the creation or production of;*
> *(c) imports or in any way takes steps to procure, obtain or access or in any way knowingly assists in, or facilitates the importation, procurement, obtaining or accessing of; or*
> *(d) knowingly makes available, exports, broadcasts or in any way distributes or causes to be made available, exported, broadcast or distributed or assists in making available, exporting, broadcasting or distributing, any film, game or publication which contains depictions, descriptions or scenes of child pornography or which advocates, advertises, encourages or promotes child pornography or the sexual exploitation of children,*
>
> *shall be guilty of an offence.*
>
> *(2) Any person who, having knowledge of the commission of any offence under subsection (1) or having reason to suspect that such an offence has been or is being committed and fails to-*
> *(a) report such knowledge or suspicion as soon as possible to a police official of the South African Police Service; and*
> *(b) furnish, at the request of the South African Police Service, all particulars of such knowledge or suspicion,*
>
> *shall be guilty of an offence.*
>
> *(3) Any person who processes, facilitates or attempts to process or facilitate a financial transaction, knowing that such transaction will facilitate access to, or the distribution or possession of, child pornography, shall be guilty of an offence.*

5.6. This position appear to have been exacerbated with the introduction into Parliament of the Films and Publications Amendment Bill 2015 [B37-2015] by the Minister of Communications on 23 November 2015 ("the FPA Bill 2015"). The FPA Bill 2015 seeks to entrench the criminalisation of "child pornography" under the Film and Publications Act 65 of 1996 ("**the FPA**"). In our view it seeks to adopt an amended definition of "child pornography" which is at

odds with that adopted in SORMAA after considerable debate regarding the decision of the Constitutional Court in the De Reuck case.

5.7. We submit that it is not desirable to have two sets of legislation setting out separate offences in respect of broadly the same conduct.

5.8. We submit that the Draft Bill should seek to delete section 24B of the FPA.

5.9. Finally – and as a general consideration – we call on the Department to use this opportunity to remove the term "child pornography" from the statute book and to substitute it with the term "Child Sexual Abuse Material" or similar. This would be in line with international practise and would also clearly indicate the intent of the adoption of the definition of "child pornography" in SORMAA, i.e. that what is being referred to has nothing to do with pornography and everything to do with evidence of the criminal abuse of a child.

_____

6. Conclusion

ISPA trusts that the above submissions will assist the Department in its deliberations around this critical process. ISPA welcomes and looks forward to more constructive interaction with the Department.

PER

ISPA REGULATORY ADVISORS

ANNEXURE A – ISPA POSTER CAMPAIGN EXAMPLES

PROTECTING CHILDREN IN CYBERSPACE

Education: Talk to your child about the risks of being online.

Awareness: Be aware of what your child is doing online.

Privacy: Teach your child not to share personal information with strangers.

To report any suspicious activities targeting children, including child sexual abuse images, please visit the Film and Publication Board's website.

www.fpbprochild.org.za

KEEP YOUR MONEY SAFE

A phishing attack is an attempt to trick you into disclosing personal information such as passwords and credit card numbers. Criminals create fake banking sites which look exactly like the real thing, and then send you an email with a link to the fake site.

If you think that you may have been the victim of a banking scam, contact your bank immediately. Contact details are available from the SABRIC web site.

Never click on a banking link in an email.
Always type in the web address of your bank yourself.

Make sure that your connection to the bank is secure – the beginning of the address will start with "https" and not "http".

Never give anyone your login details by email or over the phone.
Your bank will not ask for them in this way.

sabric www.sabric.co.za ISPA