COMMENTS BY THE LAW SOCIETY OF SOUTH AFRICA (LSSA)
ON THE CYBERCRIMES AND CYBERSECURITY BILL

The Law Society of South Africa (LSSA) wishes to take the opportunity to make the following submissions on the Cybercrimes and Cybersecurity Bill.

Introductory remarks:

The Cybercrimes and Cybersecurity Bill (the Bill) is a daunting undertaking resulting in a portmanteau of 11 chapters of draft legislation, which include chapters on definitions, offences, jurisdiction, powers to investigate, search and access or seize and international cooperation, 24/7 point of contact, structures to deal with Cybersecurity, National Critical Information infrastructure protection, evidence, general obligations of electronic communications, service providers and liability, agreements with foreign state and so on up to general provisions.

From the outset, it is clear that the inclusion of 68 sections in the Bill results in a voluminous document. It is submitted that the unnecessary duplication and incorporation of many common law principles in the Bill has contributed to the 128 pages of draft legislation that is not easy to digest.

As much as the draft legislation is considered to be generally useful and urgent, there is a need to deal with the issues raised in the Bill in detail. We request that the period for comments be extended as it appears from our assessment that the public and private sector are not fully aware of the wide implications that this draft legislation can have on our daily lives and commercial activities. There does not appear to have been the usual wide based consultation and public-private interaction in the development of this draft legislation.

It is also discomforting to note that this legislation emanates from the Justice, Crime Prevention and Security (JCPS) Cluster so is in essence a product of the State Security Agency. While the drafting of the Bill has been conducted under the auspices of the Minister of Justice and Correctional Services, it is nonetheless directed by the National Cybersecurity Policy Framework (NCPF), which is acting under the control of the State Security Agency in this instance. Several aspects of the Bill reflect, in our opinion, an unacceptable bias towards law enforcement and national security at the expense of civil liberties and hard won rights of our citizens. At the least, this aspect requires closer attention and consultation.

The general pace of development of cyber aware legislation and regulation in this country has been glacial. However, a rushed catch up attempt is unwise, although the increased awareness of the need to do something is a welcome sign. It should also be noted that the Minimum Information Security Standards (MISS), which govern information security measures within government, was first published in 1996 (almost 20 years ago). Despite the dramatic shifts in how information is communicated and processed in government, MISS, an anachronism for many years, has never been amended or replaced. Despite draft Information Security Regulations being around for many years, they remain classified and have not seen the light of day. Unfortunately, what this indicates is that even while it is stressing the urgency of cybersecurity on the one hand, government has been visibly and regrettably neglectful in establishing appropriate information security structures within its own administration. That also needs to be addressed in this process.

It is submitted that greater consultation and research should be undertaken by the Department. Furthermore, multi-stakeholder consultation is vital if this Bill is to be truly effective in the fight against cybercrime and also in increasing cybersecurity capacity and cybersecurity infrastructure. We are also not sure how much, if any, attention has been paid to the need to harmonise such legislation with that of other countries, especially in the SADC region and other African states.

It is of great concern that the Bill will be amending more than 16 already existing laws which include, but is not limited to, the South African Police Service Act of 1995, the National Prosecuting Authority Act of 1998, the Copyright Act of 1978, the Correctional Services Act of 1998, the Financial Intelligence Centre Act, 2001, the Electronic Communications and Transactions Act of 2002, the Regulation of Interception of Communications and Provision of Communication Related Information Act, 2002, the Criminal Law (Sexual Offences and Related Matters) Amendment Act, 2007, the Criminal Procedure Act 1978 and other regulations and secondary legislation. There will inevitably be unintended consequences and these must be minimised as far as possible, which will only be possible with a longer and wider period of consultation.

A Bill of this magnitude should not be rushed through Parliament and it should be able to withstand constitutional scrutiny on aspects of privacy, the right to dignity and freedom of expression. In its current state we do not believe that the Bill will pass constitutional scrutiny and it ought to be substantially revised in order to serve the purpose that it has been drafted for.

A disturbing element of the Bill is the apparent absence of the appreciation, which is a feature of all credible cybersecurity frameworks, of establishing a balance between civil liberties and the powers of national security and law enforcement agencies. There is no apparent acknowledgement of the

constitutional right of privacy, which has been globally recognised as critically important in legislative frameworks that are being developed to address 21st century issues.

The revelations of Edward Snowden have highlighted the dangers of law enforcement and national security being overzealous in the exercise of their powers. The repercussions of this can be seen in the striking down by the European Court of Justice of the Safe Harbour Accord (intended to protect the privacy of personal information of EU citizens that is processed in the USA) as a result of law enforcement overreaching its powers. If the civil liberties of citizens are ignored and the powers of national security and law enforcement (which we believe to be unconstitutional as currently provided in the Bill) are institutionalized, we are going back to earlier, darker times and run the risk of being excluded from the greater information society.

As Benjamin Franklin has observed:

"Those who give up their liberty for more security, neither deserve liberty nor security."

Specific Comments:

As much as one can ponder the various and not necessarily satisfactory definition of terms in detail, we prefer to deal with the substantive provisions of the Bill and the definition of certain terms that have either evolved or are new to the legislation can be fine-tuned later. The Bill's predecessor, the Electronic Transaction Act, Act 25 of 2002 (the ECT Act), which contained provisions about electronic writing, electronic signatures, cryptography, consumer protection, cybercrime, liability of ISPs and other related matters, has fallen behind the high speed march of technology.

Our comment is intended to focus on the Bill as a whole, as it is submitted that the Bill as it stands is unnecessarily overarching and non-exclusive to cybercrime. On the other hand, it does not adequately deal with cybersecurity issues and suggested measures to deal with risks and incidents of cybersecurity vulnerability. It also confuses the issues of cybercrime and cybersecurity, which are not synonymous although obviously related to one another.

It is submitted, for example, that the Bill does not cover all the principles as contained in the Budapest Convention on Cyber Crime (COE) and subsequent protocols and goes too far in mixing issues of cybersecurity and cyber criminality. Although the issues of cybersecurity and cyber criminality intersect, they should not be confused and given synonymous meaning. It is also concerning that it seems that the Draft International Convention to Enhance Protection from Cyber Crime and Terrorism has been completely ignored in the drafting of the Bill and the definitions of terms used.

We believe that the Bill goes in the right direction in extending the list of substantive cybercrimes that were initially limited in the ECT Act to unauthorised access to, interception of, or interference with data; making available or producing software or hardware that can overcome security measures; overcoming copyright measures, computer-related extortion, fraud and forgery; and attempting and assisting others to commit the above offences as well as spam (unsolicited commercial messages). Technology has progressed since the late 1990s and cybercrime is a much wider field with many more offences that we need to provide for.

The Bill accordingly expands the types of offences originally covered under the ECT Act and also criminalises more activities relating to the unlawful use of computer systems. The useful proposed substantive crimes include unlawful use of personal and financial information to commit offences (e.g. identity theft), use of hardware, software and computer systems to commit offences (prohibited financial transactions, e.g. phishing, spoofing and other malware related financial transactions), unauthorised access to a cyber system to steal confidential information, possession and distribution of malware as well as terrorism, espionage and extortion. It should also perhaps specifically criminalise the use of ransomware to extort money or other benefits.

It is important to consider, in a country such as South Africa that has a mixture of cultures, languages, religious beliefs and ideological backgrounds, that cyber terrorism should be better defined - something along the lines of "intentional use of or disruption or threatened disruption of any cyber or electronic system to further terrorist objectives such as civil disorder and violence". At all times, the rights of citizens should be taken into account, which is not something this Bill in its present form does.

It is suggested that Cyber Terrorism be divided into two categories, namely "effects based cyber terrorism" (which concentrates on the effects of cyber terrorism) and "intent based cyber terrorism" (which refers more to the use of any cyber system to plan and execute acts of terror, recruitment and propagation of terrorist material by e-mail and social media).

It is suggested that offences regarding cyber systems and critical infrastructure be created, as well as the criminalisation of hindrance of any cyber system's function done intentionally and systematically (DOS – Denial of Service Attacks). It is also suggested that the crime of interfering with a cyber system with intent to do harm to data or cause substantial damage and all other forms of malicious conduct targeted against a state and its inhabitants be criminalised.

Penalties proposed on conviction include fines of up to R5 million or R10 million and imprisonment of up to five or 10 years, depending on the severity of the offence. Offences against the state carry penalties of up to 25 years' imprisonment. This is welcomed and will go some way to deter cyber

criminals, especially those who would go “forum shopping” for jurisdictions where cybercrimes would not be punished as severely as in others.

It is submitted that the provisions relating to infringement of copyright (e.g. re-posting an article on a blog without permission or acknowledgement) should not have been included in the Bill, as they have been already extensively covered in the Copyright Act Review which is currently being undertaken by the Department of Trade and Industry. “To sell, offer for download, distribute or otherwise make available a copyright work online” covers almost anything that can be done with a copyright work online, other than up or downloading it for personal use.

The section dealing with jurisdiction is as confusing, if not more so, than its predecessor set out in the ECT Act and has muddied the waters even more in the international law milieu where jurisdiction has been considered a long standing and unresolved vexed issue – especially when two different jurisdictions claim jurisdiction over any act of cyber criminality.

The proposed section dealing with search and access or seize and international cooperation has its own difficulty. Some of the provisions for using in the search and seizure of real time e-evidence display a draconian tone and would allow excessive government and law enforcement intrusion into legitimate expectations of privacy and anonymity. Search for and access to or seizure of certain articles (it is assumed hardware and software) by way of an oral application for a search warrant or amendment of an existing warrant makes it easier for law enforcement to get access to the real-time computer evidence required. This is a sensible step in dealing with the legal lacunae that existed in the Criminal Procedure Act, which only dealt with access to documents, but of which the application was later extended to computer data. This will also result in a currently much needed expedited preservation of e-evidence, but must be carefully used in the light of constitutional rights to privacy and the right to dignity, as well as freedom of expression.

The inclusion of a provision relating to e-evidence directions for its preservation and the fact that oral application for such preservation directions is proposed is seen as in line with international best practice, but must once again be balanced with the individual’s right to privacy, the right to dignity and the right to freedom of expression as enshrined in our Constitution. It is interesting that the Bill proposes a section dealing with the admissibility of electronic evidence obtained as result of a direction requesting foreign assistance and cooperation. However, one would have thought that such would have been adequately covered in the Review of the Law of Evidence project already being dealt with by the South African Law Reform Commission. It seems that there has not been sufficient or any attention paid to other projects which cover similar ground. This should be corrected.

Although some companies may argue that they must preserve customer confidentiality, it is sensible that Electronic Communications Service Providers (ECSPs) will have a general obligation to keep, monitor, disclose and produce customer information (traffic data and in certain cases regarding the actual user) to law enforcement under certain conditions. The judicial oversight of such disclosures should however be recognised and emphasised in light of the right to privacy, the right to dignity and the right to freedom of expression as enshrined in our Constitution.

It is also refreshing that the Bill proposes issuing of directions requesting foreign assistance and cooperation which is re-stated in the Budapest Convention as well as the African Union Cyber Security Convention. We are however concerned about the efficacy of the many structures of cybersecurity that are envisaged in the Bill, due to budgetary constraints that we have in South Africa.

The Bill proposes the following structures:

A Cyber Response Committee, a Cyber Security Centre, Government Security Incident Response Teams (which currently exist), a National Cybercrime Centre (we hope that this centre will be placed within the SA Police Service and the Hawks), a Cyber Command (which we hope will be placed with State Security and South African Defence).

“Cyber warfare” is a new battlefield compared to the traditional war battlefield but no less real for that. It is difficult to regulate cyber warfare as it crosses jurisdictions and is not regulated and although mention of a Cyber Command is made, we believe that the Bill does not adequately deal with the very real threats of cyber warfare and cyber-attacks.

The Bill also suggests the creation of Private Sector Security Incident Response Teams. We have yet to see the relevance and performance of the new cyber security hub which is currently hosted at the CSIR and seems to have been included in the draft Bill. There are some other novel attempts to deal with national critical information infrastructures protection, such as the identification and declaring of National Critical Information Infrastructures, the establishment and control of a National Critical Information Infrastructure Fund, as well as the inspection of National Critical Information Infrastructures to ensure compliance, but some of the novelty does not reach actual practicality. All these structures will need to be supported by proper funding and sufficient capacity.

We are of the view that this Bill is inelegantly drafted and flawed, does not take basic constitutional rights properly into account and suffers from a lack of proper consultation. We suggest that the Bill be revised and reworked with regard to all comments received from the public and private sector, as well as the legal profession and information security practitioners.

We suggest that, once the comments have been received, a workshop be organised to discuss them. Any fast tracking of the Bill in its current form will have serious implications, may expose the Bill to constitutional challenges in Court and may derail the bona fide intentions of the legislature to further regulate cyber criminality and aspects of cybersecurity. The legal profession would willingly participate in further consultations and has many expert members who can contribute meaningfully to this development process.

The Bill should also be trimmed to avoid duplication of provisions already contained in other legislation and avoid the re-inventing of the wheel by codifying common law principles and crimes. We would like to be proactively involved in the further development of the Bill, which we also believe should happen on as urgent a basis as possible.