Myanmar: Digital Content Proposals[1]

January 2018

1. Introduction

The Centre for Law and Democracy (CLD), working with its local partner, the Myanmar Media Lawyers' Network (MMLN), and other local organisations, has hosted a number of discussions and workshops on legal provisions in Myanmar which unduly limit freedom of expression in the digital space. Reform efforts led, in August 2017, to some procedural reforms relating to one of the most problematical and widely used provisions – section 66(d) of the 2013 Telecommunications Law – but no substantive changes to this or other provisions have so far been made.

Part of the problem may have been that the campaign only focused on one of the problematical provisions, while part may have been that parliament felt uncomfortable simply repealing a provision without adopting any alternative or replacement.

To address these concerns, this note sets out our initial thinking on how to amend key provisions to bring them more closely into line with international standards for three laws, namely the Official Secrets Act, 1923, the 2004 Electronic Transactions Law, and the 2013 Telecommunications Law. For each law, the note provides the existing provisions and then sets out our proposals for reform, along with a short explanation.

We intend to conduct discussions among key stakeholders in Myanmar with a view to improving these proposals and making sure they are responsive to local needs. We then aim to work with local stakeholders to try to get the proposals adopted into law.

2. The Official Secrets Act

Existing Provisions

3.(1) If any person for any purpose prejudicial to the safety or interests of the State-

(a) approaches, inspects, passes over or is in the vicinity of, or enters, any prohibited place; or

(b) makes any sketch, plan, model, or note which is calculated to be or might be or is intended to be, directly or indirectly, useful to an enemy; or

(c) obtains, collects, records or publishes or communicates to any other person any secret official code or password, or any sketch, plan, model, article or note or other document or information which is calculated to be or might be or is intended to be, directly or indirectly, useful to an enemy;

he shall be punishable with imprisonment for a term which may extend, where the offence is committed in relation to any work of defense, arsenal, naval, military or air force establishment or station, mine, minefield, factory, dockyard, camp, ship or aircraft or otherwise in relation to the naval, military or air force affairs of [the State]1 or in relation to any secret official code, to fourteen years and in other cases to three years.

(2) On a prosecution for an offence punishable under this section with imprisonment for a term which may extend to fourteen years, it shall not be necessary to show that the accused person was guilty of any particular act tending to show a purpose prejudicial to the safety or interests of the State, and, notwithstanding that no such act is proved against him, he may be convicted if, from the circumstances of the case or his conduct or his known character as proved, it appears that his purpose was a purpose prejudicial to the safety or interests of the State; and if any sketch, plan, model, article, note, document, or information relating to or used in any prohibited place, or relating to anything in such a place, or any secret official code or pass word is made, obtained, collected, recorded, published or communicated by any person other than a person acting under lawful authority, and from the circumstances of the case or his conduct or his known character as proved it appears that his purpose was a purpose prejudicial to the safety or interests of the State, such sketch, plan, model, article, note, document or information shall be presumed to have been made, obtained, collected, recorded, published or communicated for a purpose prejudicial to the safety or interests of the State.

5.(1) If any person having in his possession or control any secret official code or password or any sketch, plan, model, article, note, document or information which relates to or is used in a prohibited place or relates to anything in such a place, or which has been made or obtained in contravention of this Act, or which has been entrusted in confidence to him by any person holding office under Government, or which he has obtained or to which he has had access owing to his position as a person who holds or has held office under Government, or as a person who holds or has held a contract made on behalf of Government, or as a person who is or has been employed under a person who holds or has held such an office or contract-

(a) wilfully communicates the code or password, sketch, plan, model, article, note, document or information to any person other than a person to whom he is authorized to communicate it, or a Court of Justice or a person to whom it is, in the interests of the State, his duty to communicate it; or

(b) uses the information in his possession for the benefit of any foreign power or in any other manner prejudicial to the safety of the State; or

(c) retains the sketch, plan, model, article, note or document in his possession or control when he has no right to retain it, or when it is contrary to his duty to retain it, or wilfully fails to comply with all directions issued by lawful authority with regard to the return or disposal thereof; or

(d) fails to take reasonable care of, or so conducts himself as to endanger the safety of, the sketch, plan, model, article, note, document, secret official code or pass word or information;

he shall be guilty of an offence under this section.

(2) If any person voluntarily receives any secret official code or password or any sketch, plan, model, article, note, document or information knowing or having reasonable ground to believe, at the time when he receives it, that the code, pass word, sketch, plan, model, article, note, document or information is communicated in contravention of this Act, he shall be guilty of an offence under this section.

(3) If any person having in his possession or control any sketch, plan, model, article, note, document or information which related to munitions of war, communicates it, directly or indirectly, to any foreign power or in any other manner prejudicial to the safety or interests of the State, he shall be guilty of an offence under this section.

(4) A person guilty of an offence under this section shall be punishable with imprisonment for a term which may extend to two years, or with fine, or with both.

Our Proposals

3.(1) If any person, intentionally and without legal authorisation, and for any purpose which is prejudicial to the security of the State, -

Note: The requirements of intention and an absence of legal authorisation have been added. The former is normal in criminal matters and the latter protects those who act under legal authority. The scope of this has also been narrowed down to proper State security issues (which have also been defined – see sub-section 3(3) below).

(a) inspects or enters any prohibited place; or

Note: The references to "approaches", "passes over" and "in the vicinity of" have been removed as being unrealistic and overbroad. "Inspection" will cover all activities which are actually harmful.

(b) [Repealed]

Note: There is no need for a separate sub-section here. This has been added to (c) below.

(c) makes, obtains, collects, records or publishes or communicates to any other person any secret official code or password, or any sketch, plan, model, article or note or other document or information which is intended to be and is in fact likely to cause harm to national security;

Note: The requirement of intention has been added. The references to "calculated to be", "might be" and "directly or indirectly" have been removed and replaced with a requirement of likelihood. The idea of being useful to an enemy has also been replaced by the broader notion of national security. This will provide adequate protection to national security while also respecting freedom of expression.

he shall be punishable with imprisonment for a term which may extend, where the offence is committed in relation to any work of defence, arsenal, naval, military or air force establishment or station, mine, minefield, factory, dockyard, camp, ship or aircraft or otherwise in relation to the naval, military or air force affairs of the State

or in relation to any secret official code, to seven years and in other cases to three years.

Note: The maximum penalty here has been reduced to seven years so as to be more in line with the nature of the crime.

(2) [Repealed]

Note: This sub-section has been repealed. It effectively removes the intent requirement which is contrary to basic principles of criminal law and also substantially increases the risk of abuse of this provision.

(3) For purposes of this section, a purpose is prejudicial to the security of the State if a person-

(a) commits, in Myanmar, an offence against the laws of Myanmar that is punishable by a maximum term of imprisonment of two years or more in order to advance a political, religious or ideological purpose, objective or cause or to benefit a foreign entity or terrorist group;
(b) commits, inside or outside Myanmar, a terrorist activity;
(c) causes or aggravates an urgent and critical situation in Myanmar that threatens the ability of the Government of Myanmar to preserve the sovereignty, security or territorial integrity of Myanmar;
(d) impairs or threatens the military capability of the Armed Forces of Myanmar, or any part of those Forces;
(e) interferes with the design, development or production of any weapon or defence equipment of, or intended for, the Armed Forces of Myanmar, including any hardware, software or system that is part of or associated with any such weapon or defence equipment;
(f) impairs or threatens the capabilities of the Government of Myanmar in relation to security and intelligence; or
(g) impairs or threatens the capability of the Government of Myanmar to conduct diplomatic or consular relations, or conduct and manage international negotiations.

Note: This sub-section has been added to clarify the scope of State security for purposes of this section.

5.(1) If any person having in his possession or control any secret official code or password or any sketch, plan, model, article, note, document or information which has legitimately been classified as secret on the basis that its disclosure would pose a serious risk of harm to national security and which has been entrusted in confidence to him by any person holding office under Government, or which he has obtained or to which he has had access owing to his position as a person who holds or has held office under Government, or as a person who holds or has held a contract made on behalf of Government, or as a person who is or has been employed under a person who holds or has held such an office or contract-

Note: The ideas of information that "relates to or is used in a prohibited place", "relates to anything in such a place", "which has been made or obtained in contravention of this Act" or which is simply held as a result of a person's position have been replaced by the idea that the information must have

legitimately been classified as secret and be held by the person as a result of his or her position.

(a) wilfully communicates the code or password, sketch, plan, model, article, note, document or information to any person other than a person to whom he is authorised to communicate it, or a Court of Justice or a person to whom it is, in the interests of the State, his duty to communicate it; or

Note: No change has been made to this provision.

(b) wilfully uses the information in his possession in any manner which is prejudicial to national security; or

Note: The ideas of using information "for the benefit of any foreign power" and against "the safety of the State" have been replaced by the idea of prejudice to national security. A requirement of wilfulness has been added to reflect the need for a mental element for every crime.

(c) wilfully retains the sketch, plan, model, article, note or document in his possession or control when he has no right to retain it, or when it is contrary to his duty to retain it, or wilfully fails to comply with all directions issued by lawful authority with regard to the return or disposal thereof; or

Note: The defence of wilfulness has been expanded to all of this sub-section, on the basis that all crimes should involve a mental element.

(d) fails to take reasonable care of, or so conducts himself as to endanger the safety of, the sketch, plan, model, article, note, document, secret official code or pass word or information;

Note: No change has been made to this provision.

he shall be guilty of an offence under this section.

(2) [Repealed]

Note: This is simply not reasonable. It is no fault of a person if they receive secret information. Furthermore, where information is provided in the public interest, the person should receive it.

(3) [Repealed]

Note: This is already covered by sub-section 5(1)(a).

(4) A person guilty of an offence under this section shall be punishable with imprisonment for a term which may extend to two years, or with fine, or with both.

Note: No change has been made to this provision.

5A. Where the offences in sections 3 and 5 involve expressive activity they shall not apply where it is established that the person involved acted in the public interest.

Note: This sort of public interest defence for expression crimes is necessary to balance the protection of national security and other interests with the right to freedom of expression.

3. The Electronic Transactions Law

Existing Provisions

33. Whoever commits any of the following acts by using electronic transactions technology shall, on conviction be punished with imprisonment for a term which may extend from a minimum of 7 years to a maximum of 15 years and may also be liable to a fine:

(a) doing any act detrimental to the security of the State or prevalence of law and order or community peace and tranquillity or national solidarity or national economy or national culture.

(b) receiving or sending and distributing any information relating to secrets of the security of the State or prevalence of law and order or community peace and tranquillity or national solidarity or national economy or national culture.

34. Whoever commits any of the following acts shall, on conviction be punished with imprisonment for a term which may extend to 5 years or with fine or with both:

(a) sending, hacking, modifying, altering, destroying, stealing, or causing loss and damage to the electronic record, electronic data message, or the whole or part of the computer programme dishonestly;

(b) intercepting of any communication within the computer network, using or giving access to any person of any fact in any communication without permission of the originator and the addressee;

(c) communicating to any other person directly or indirectly with a security number, password or electronic signature of any person without permission or consent of such person;

(d) creating, modifying or altering of information or distributing of information created, modified or altered by electronic technology to be detrimental to the interest of or to lower the dignity of any organization or any person.

38. Whoever attempts to commit any offence of this Law or conspires amounting to an offence or abets the commission of an offence shall be punished with the punishment provided for such offence in this Law.

Our Proposals

33. Whoever commits any of the following acts by using electronic transactions technology shall on conviction be punished with imprisonment for a term which may extend to a maximum of 7 years or with a fine or with both:

(a) carrying out any act with the intention and likely effect of posing a serious risk of harm to national security or to the maintenance of law and order.

Note: The minimum penalty has been removed (these are highly problematical outside of offences which are always very serious such as murder or rape) and a lower maximum penalty has been added to reflect the level of seriousness of the crime. The requirements of intent and creating an actual risk of serious harm have been added. References to "community peace and tranquillity or national solidarity or national economy or national culture" have been removed as being overbroad and unnecessary.

(b) distributing any information which is identified as secret with the intention

and likely effect of posing a serious risk of harm to national security or to the maintenance of law and order.

Note: As with the previous provision, the requirements of intent and creating an actual risk of serious harm have been added. Once again, references to "community peace and tranquillity or national solidarity or national economy or national culture" have been removed as being overbroad and unnecessary.

34. Whoever commits any of the following acts by using electronic transactions technology shall on conviction be punished with imprisonment for a term which may extend to 5 years or with a fine or with both:

(a) hacking, modifying, destroying, or causing damage to an electronic record, an electronic data message or the whole or part of a computer programme in the absence of any express or implied authorisation and with the intent of causing harm to the legitimate interests of a third party;

Note: Stealing is already a crime pursuant to the Penal Code, for example, sections 378-382. Sending has been removed because this is not a new (digital) phenomenon and the rare cases in which it might be illegal (such as because it is a threat or an attempt to blackmail) are already addressed in the Penal Code. 'Altering' is already covered by 'modifying' and the notion of 'causing loss' is covered by 'causing damage'. The defences of having authorisation and the need to cause harm to the legitimate interests of a third party have been added, and the intent requirement has been clarified.

(b) intercepting of any private communication within the computer network, using or giving access to any person of any fact in any private communication in the absence of any express or implied authorisation and in a way that poses a serious risk of harm to the legitimate interests of a third party, including privacy; and

Note: The scope of this has been limited to private communications, since it is legitimate to distribute public communications. The requirement of permission has been replaced by the idea of an absence of either express or implied authorisation. It is clearly not reasonable to require permission to send someone an email; implied authorisation is enough. A requirement of causing harm to the legitimate interests of a third party has also been added since even an unauthorised action which fails to cause any harm should not be punished.

(c) communicating to any other person directly or indirectly a security number, password or electronic signature of any person in the absence of any express or implied authorisation and in a way that poses a serious risk of harm to the legitimate interests of a third party, including privacy.

Note: The requirement of permission or consent has been replaced by the idea of an absence of either express or implied authorisation. Forwarding emails often involves forwarding a digital signature and this should not require permission; implied authorisation is enough. As with the previous provision, a requirement of causing harm to a legitimate interest has also been added.

(d) [Repealed in favour of section new 34A]

34A. The distribution of content to third parties using electronic transactions technology shall be deemed to be included within the meaning of the phrase ''makes

or publishes" found in section 499 of the Penal Code.

> Note: Section 34(d), creating a separate sort of defamation offence, has been repealed and replaced with a new section 34A, which makes it clear that disseminating content using electronic transactions technology is also covered by the defamation provisions in the Penal Code.

38. Whoever attempts or conspires to commit any of the offences set out in this Law in a way that amounts to an offence or abets the commission of an offence shall be liable to the punishment provided for in this Law for such offence, provided that the mere provision of electronic services shall not be deemed to constitute an attempt, conspiracy or abetting, unless it is done with that specific intention.

> Note: A defence has been added here for service providers who merely provide electronic services, unless they act with the specific intent of attempting, conspiring to commit or abetting a crime.

38A. Where the offences in sections 33(a) and (b) and 34(a), (b) and (c) involve expressive activity they shall not apply where it is established that the person involved acted in the public interest.

> Note: This sort of public interest defence for expression crimes is necessary to balance the protection of national security and other interests with the right to freedom of expression.

4. The Telecommunications Law

Existing Provisions

66. Whoever commits any of the following acts shall, on conviction, be liable to imprisonment for a term not exceeding three years or to a fine or to both.

…

> (c) Stealing, cheating, misappropriating or mischief of any money and property by using any Telecommunications Network.
> (d) Extorting, coercing, restraining wrongfully, defaming, disturbing, causing undue influence or threatening to any person by using any Telecommunications Network.

68. Whoever commits any of the following acts shall, on conviction, be liable to imprisonment for a term not exceeding one year or to a fine or to both.

> (a) communications, reception, transmission, distribution or conveyance of incorrect information with dishonesty or participation;

69. Whoever, unless for the matters concerning prosecution regarding Telecommunications, and unless authorized under court order to disclose, discloses any information which is kept under a secured or encrypted system to any irrelevant person by any means shall, on conviction, be liable to imprisonment for a term not exceeding one year or to a fine or to both.

73. Whoever attempts to commit any offence under this Law, or conspire or abets the commission of an offence shall be liable to the punishment provided in this Law for such offence.

75. The Union Government may, as may be necessary, direct to the relevant organization for enabling to obtain any information and telecommunications which causes harm to national

security and prevalence of law without affecting the fundamental rights of the citizens.

77. The Ministry may, when an emergency situation arises to operate for public interest, direct the licensee to suspend a Telecommunications Service, to intercept, not to operate any specific form of communication, to obtain necessary information and communications, and to temporarily control the Telecommunications Service and Telecommunications Equipments.

Our Proposals

66. Whoever commits any of the following acts shall, on conviction, be liable to imprisonment for a term not exceeding three years or to a fine or to both.

…

(c) [Repealed in favour of section new 66A]
(d) [Repealed in favour of section new 66A]

66A. The use of a telecommunications network to steal, cheat, misappropriate, cause mischief to money or property, extort, coerce, wrongfully restrain, defame or threaten a person shall be deemed to be included as a means of committing these crimes within the meaning of the relevant provisions in the Penal Code.

Note: Sections 66(c) and (d), creating various crimes, have been repealed and replaced with a new section 66A, which makes it clear that carrying out these actions using a telecommunications network is covered by the relevant provisions in the Penal Code.

68. Whoever commits any of the following acts shall, on conviction, be liable to imprisonment for a term not exceeding one year or to a fine or to both.

(a) [Repealed]

…

Note: Section 68(a) has been repealed. The Penal Code already provides for a number of specific offences relating to dishonestly disseminating incorrect information, such as fraud and blackmail, and it is not legitimate to impose a blanket ban on this sort of information.

69. Whoever by any means discloses any information which is kept under a secured or encrypted system to any third person with the intention of and in a way that actually poses a serious risk of causing harm to the legitimate interests of another third party, including privacy, in the absence of any express or implied authorisation, or unless for matters concerning prosecution regarding Telecommunications as authorised by a court order, shall, on conviction, be liable to imprisonment for a term not exceeding one year or to a fine or to both.

Note: The defences of having authorisation and the need to cause harm to the legitimate interests of a third party have been added, and an intent requirement has been added.

73. Whoever attempts or conspires to commit any of the offences set out in this Law in a way that amounts to an offence or abets the commission of an offence shall be liable to the punishment provided for in this Law for such offence, provided that the mere provision of telecommunications services shall not be deemed to constitute an attempt, conspiracy or abetting, unless it is done with that specific intention.

Note: A defence has been added here for service providers who merely provide telecommunications services, unless they act with the specific intent of attempting, conspiring to commit or abetting a crime.

73A. Where the offences in sections 66A, 69 and 73 involve expressive activity they shall not apply where it is established that the person involved acted in the public interest.

Note: This sort of public interest defence for expression crimes is necessary to balance the protection of national security and other interests with the right to freedom of expression.

75. A court may authorise relevant Union Government officials or organisations to intercept information and/or telecommunications where necessary to protect national security or the maintenance of law and order against a serious risk of harm, as long as this does not undermine the fundamental rights of citizens.

Note: A requirement to obtain court authorisation for the interception of information has been added, as this is a normal requirement for this sort of State action. The condition of protecting against a serious risk of harm has also been added.

77. [Repealed]

Note: This provision has been repealed. Experience in countries around the world clearly demonstrates that it is not necessary for government to wield this sort of power. Where necessary, a court may, under section 75, authorise an information intercept. And, where a telecommunications service provider is acting illegally or causing harm, courts can also act urgently to take action under laws such as the Penal Code.