Myanmar

Analysis of Draft Cyber Security Law

February 2021

Centre for Law and Democracy
info@law-democracy.org
+1 902 431-3688
www.law-democracy.org

Table of Contents

Introduction[1]

A draft Cyber Security Law (draft Law) has been circulated by the military regime which is currently governing Myanmar, following the coup d'état in early February. According to an apparently official announcement by the Ministry of Transport and Communication on 9 February 2021,[2] comments on the draft are requested by 15 February 2021. This Analysis has been prepared on an urgent basis by the Centre for Law and Democracy (CLD) with a view to helping local stakeholders understand the problems with the draft Law from the perspective of international human rights law.

This Analysis focuses on the human rights implications of the draft Law, with a particular focus on freedom of expression and privacy. As such, it does not address a number of other potential problems such as practical challenges in implementing it or the costs involved. The Analysis also does not address the question of whether or not it is legitimate in the first place for the military regime to adopt a law along these lines, or indeed any law, a point which has been made by some commentators.[3] Instead, it focuses only on the content of the draft Law. We do note, however, that for a law with profound implications for human rights, the period given for comments, of just six days, is seriously insufficient.

Due to the very brief timeframe for making comments, our Analysis is based on a very rapidly completed unofficial translation of the draft Law.[4] The Analysis was also completed very quickly, so as to provide inputs to local stakeholders before the end of the short period for providing comments on the draft Law. As a result, while it is based on international standards, it does not generally provide references or links to those standards. CLD is ready to provide anyone who is interested with detailed references to relevant international standards upon request.

Myanmar has been discussing and working on a cyber law for quite some time now, with the support of the World Bank and the Singapore-based consulting firm, TRCP. The current draft Cyber Security Law is, however, much narrower in focus than the earlier effort and it is unclear whether and to what extent it draws on that earlier work.

---

[2] Reference: 500-Has Nya/Khwe (5) license/1873, 9 February 2021.

[3] See Civil Society Statement on the so-called "Cyber Security Bill", 10 February 2021, http://freeexpressionmyanmar.org/civil-society-statement-on-the-so-called-cyber-security-bill-အာဏာသိမ်း-စစ်အ/.

[4] CLD takes no responsibility for any weaknesses in our Analysis which arise from errors in the translation.

This Analysis focuses on six issue areas in the draft Law, namely the independence and powers of the institutional structures created by the draft Law, the rules on personal data protection and data storage, restrictions on the content of what may be shared online, other criminal rules in the draft Law, the burdens placed on private sector actors (important from a freedom of expression perspective since many of these actors serve to facilitate or enable online speech), and critical information infrastructure. The analysis itself is drawn from international human rights standards, for example as set out in the *Universal Declaration of Human Rights* (UDHR),[5] adopted in 1948. As a United Nations General Assembly resolution, the UDHR is not directly binding on States but its preeminent status as a statement of international human rights and the fact that States rarely if ever repudiate at least some of its principles means that those principles, including its guarantees of freedom of expression and privacy, have very likely acquired legal force as customary international law.[6]

1. Institutional Structures: Independence and Powers

The draft Law creates four main institutional structures. At the top of the pyramid is the Cyber Security Central Committee (Central Committee), appointed by the State Administration Council, which was itself created on 2 February 2021 to serve as the peak executive body in Myanmar under the new governing arrangements. The Chair of the State Administration Council and the Minister of the Ministry responsible for cyber security serve as co-chairs of the Central Committee, which also draws members from among other ministers and a secretary appointed by the State Administration Council (section 5(a)). The Central Committee is thus entirely controlled by the executive.

The Cyber Security Executive Committee (Executive Committee), in turn, is appointed by the Central Committee, with the approval of the State Administration Council. The Minister of the Ministry responsible for cyber security serves as the chair, with members being drawn from among deputy ministers or permanent secretaries of different ministries, cyber security professionals and representatives of non-governmental organisations (section 9). Although the Executive Committee does include non-government representatives, its appointment by the Central Committee gives the executive control over it. Furthermore, both the Central Committee and the Executive Committee are served by a secretariat which is "determined" by the State Administration Council, which performs under the supervision of the Ministry responsible for cyber security and which is responsible for the work of both Committees (sections 7 and 8). This further cements the executive's control over the Executive Committee.

Third, the Executive Committee, with the agreement of the Central Committee, shall form Working Committees, at least in the areas of Cyber Security, Cyber Crimes and Cyber Protection

[5] United Nations General Assembly Resolution 217A (III), 10 December 1948.
[6] See, for example, D'Amato, A., "Human Rights as Part of Customary International Law: A Plea for Change of Paradigms" (2010, Faculty Working Papers, 88), https://scholarlycommons.law.northwestern.edu/facultyworkingpapers/88; and Meron, T., *Human Rights and Humanitarian Norms as Customary Law* (1989, Oxford, Clarendon Press).

(section 11). Finally, the Executive Committee, again with the agreement of the Central Committee, shall form investigation teams as needed (section 12).

It is legitimate for government-controlled bodies to undertake policy work, even where that impacts on human rights such as freedom of expression. However, international standards call for any direct regulation or implementation of policy which affects freedom of expression to be done by actors which are independent of government. Otherwise, political considerations are likely to influence regulatory decisions, rather than being made in the overall public interest, which will then undermine the free flow of information and ideas in society (i.e. freedom of expression). The Central Committee, in particular, does undertake a number of policy tasks. However, its duties also include direct regulatory responsibilities. For example, pursuant to section 6(h) of the draft Law, it is responsible for the following:

> Inform, restrict and limit local and international cyber security service provider operators and organisations to act in accordance with the cyber security guidelines and programs of critical information infrastructures.

Section 6(g) is even more intrusive, providing for the Central Committee to:

> In order to effectively implement objectives contained in this law, determine the information storage of business and operators from the online communication sector in which the public engages through national cyber space.[7]

The regulatory powers of the Executive Committee are even more explicit, as it "permits, rejects, and sanctions of the license of services" under the law (section 10(k)) and also "scrutinises and permits cyber security teams or organisations" and sanctions those formed without permission (section 10(o)).

The exercise of these sorts of regulatory powers by bodies which are not independent of government, as is the case with the Central Committee and Executive Committee, is not legitimate according to international law.

Beyond these general regulatory powers, specific powers are allocated to different institutional structures which are very intrusive in nature. Sections 43, 45 and 46 allocate broad and fairly undefined powers to the three mandatory Working Committees. For example, under section 43(b), they are tasked with "preventing any other consequences of cyber security threats, cyber attacks, cyber terrorism, cyber fraud, or cyber incidents from occurring", while under section 43(e) they are tasked with "Investigating and taking actions against" these sorts of threats.

It is not exactly clear how far these powers go, but they at least extend to inspecting the computers not only of anyone considered to be directly "related to" any of these threats, but also of any other party who is "related with" the first party, subject only to an obligation to return the computer after assessing it (sections 45 and 46). These are extensive and highly intrusive powers

[7] Note that there are two versions of section 6(g) in the translation we are using, one before section 6(h) and one after. This is the second one.

which do not appear to be subject to any form of constraint apart from the one about the individual involved being "related" to an attack (although even this extends to anyone who is just "related with" that first person). This may be contrasted with human rights standards about police investigations, which subject them to important constraints of both a procedural nature (for example often requiring the prior approval of a judge) and a substantive nature (for example that there is a clear link between the investigation and gathering necessary evidence relating to a crime).

Similarly unconstrained powers are placed in the hands of investigation teams. Section 47 authorises the State Administration Council to grant any person or organisation the power to conduct investigations under existing laws (this appears to be in addition to the investigation teams appointed by the Executive Committee pursuant to section 12). Section 49 does at least require these actors not to interfere with "the fundamental rights of the citizens", but otherwise grants them very broad and again apparently entirely unconstrained powers, such as to prevent "issues that can harm the sovereignty and territorial integrity of the State" (section 49(a)), perform "acts of rule of law and public order" (section 49(c)) and investigate crimes (section 49(d)). Similarly, pursuant to sections 52 and 53, the "inspection body" can seize evidence to inspect it and submit it to the court, again apparently without any constraints.

Pursuant to section 50, the Ministry, the Department (which is defined as the one serving as the secretariat of the Central and Executive Committees) or organisation it may authorise can "visit and check and oversee the site of any online service provision business" where this is considered to be necessary to protect either State security or just the "public interest", whatever that may be deemed to cover. Section 51 is even more draconian, authorising the Ministry, where necessary, again in the "public interest", to temporarily suspend the provision of any online service, temporarily control any device relating to the provision of online services or even permanently terminate an online service provision business. These are powers that should only be wielded by a court or potentially an independent regulator which is subject to judicial oversight, and according to strict and clear conditions, such as a serious breach of licence conditions or the law. The open-ended term "public interest" should never be grounds for exercising such intrusive powers as these.

Section 72 also provides for sanctions to be imposed by the Department which range from a warning to a fine to temporary or permanent suspension of an online service or business licence. Here again, these sorts of powers should never be placed in the hands of executive actors although the conditions for imposing such sanctions are more clearly defined, namely a breach of sections 44 or 48 of the draft Law, relating to collaborating with Working Committees and investigators.

The exercise of these powers is not even subject to an independent right of appeal. Pursuant to sections 76 and 77, anyone who is aggrieved by the exercise of these powers may appeal only to the (executive-controlled) Central Committee, the decisions of which "shall be conclusive and final".

Taken together, the complete lack of independence of the institutional structures under the draft Law, the extremely extensive and largely unconstrained powers granted to them to investigate, seize evidence and even impose sanctions, and the barring of any appeal to an independent body, apparently including the courts, constitute serious breaches of both due process rights and, given the fact that many of those subject to these measures will be involved in facilitating online communications, the right to freedom of expression.

Recommendations:

- The Central and Executive Committees should either not have any direct regulatory powers or they should be transformed into bodies that are independent of government.
- The powers that these bodies and the bodies that operate under them wield should be subject to appropriate both substantive and procedural conditions, along the lines of the constraints to which similar powers exercised by analogous actors, such as the police, are subject to in rule of law systems.
- The power to impose more intrusive sanctions, such as suspensions or terminations of service, should be subject to particularly limiting conditions.
- The imposition of the sorts of measures in the hands of the Central and Executive Committees, including sanctions, on private sector actors should always include a right of appeal to the courts.

2. Personal Data Protection and Data Storage Rules

Myanmar does not currently have a data protection regime or even a proper set of rules on the protection of privacy, although these are both a key part of protecting basic human rights, in particular the right to privacy. Sections 13-15 of the draft Law, along with the sanctions envisaged in sections 56-57, create a very basic system of data protection. Section 13 calls on what are commonly referred to as "data controllers" to "systematically keep, protect and manage the personal information" in accordance with the law, along with a few more specific rules, such as destroying personal data once it is no longer needed. Section 14 also requires investigation teams to respect the confidentiality of personal data, subject to the law. Articles 56 and 57 provide for sanctions for data controllers who do not respect the rules and for others who interact in various ways with personal data without approval.

This only begins to scratch the surface of what would constitute a proper personal data protection regime. A properly developed system would, among other things, place far more detailed obligations on data controllers, define precise and narrow exceptions to data protection principles, create a number of direct rights for data subjects (those to whom the data relates), including to inspect and correct or require the deletion of data in appropriate cases, and create an independent and empowered administrative oversight body to enforce the rules.

Furthermore, section 15 carves out a number of very broad exceptions from even these limited general data protection obligations. These cover a wide range of functions that the draft Law addresses, such as prevention, search, enquiry, investigation, data collection, information sharing and coordination relating to cyber security and various other cyber risks. While every country recognises some limitations to personal data protection rules for purposes of the administration of justice, these need to be clearly and appropriately defined, which is not the case here.

The introduction of any data protection rules for Myanmar could be seen as a move in the right directly. However, this would not be the case if this were in any way to serve as a barrier to the adoption of a proper data protection system, which Myanmar urgently needs to do.

Section 28(a) of the draft Law calls on Internet service providers "in Myanmar" to ensure that users' data is stored "in a place designated by the Ministry". It is not clear how the Ministry might go about designating places for data storage but this sort of language is usually used to refer to requirements to host data locally (i.e. within the jurisdiction). While many countries have some local data storage requirements, the potential scope of this obligation under the draft law is very broad indeed. Internet service providers are defined in section 3(u) as including any "person or any business providing the online service to be used in Myanmar", while section 3(t) defines an "online service" very broadly to include any service provided online using digital equipment. If applied broadly by the Ministry, these rules would make it impossible for many service providers, including the social media platforms which provide essential services to enable freedom of expression, to operate in Myanmar. Better practice would be to set much more precise and limited rules and conditions for the designation of data storage places by the Ministry. At a minimum, the Ministry should go about this task in a manner that does not threaten the ability of communication service providers to operate effectively.

The draft Law sets strict rules on data retention by Internet service providers, with Section 30 requiring an extensive range of user data to be retained for "up to three years" (which we understand as meaning for three years, since otherwise one day qualify as "up to three years"). This includes name, address and ID details of the user, the service record of the user (which could include telephone metadata for phone service providers – which numbers were called, for how long and potentially even from where – or browsing history for Internet access providers) and any other information the Department requires. International law has quite clear standards in this area which prohibit the imposition of mass data retention requirements on service providers (beyond what is needed for commercial purposes). Such requirements breach the right to privacy and potentially also the presumption of innocence.

Section 31 then requires Internet service providers to provide this data to an "assigned person or authorised organisation requested under any existing law". The legitimacy of this depends on the conditions in other laws for requiring third parties to provide private data to authorised bodies, which is beyond the scope of this Analysis. However, international law establishes strict conditions for accessing this sort of information. Furthermore, extensive experience in countries around the world shows that it is very difficult to ensure respect even for legal provisions in this space, which is another reason why mass data retention rules are not legitimate in the first place.

Recommendations:

- Myanmar should adopt a fully developed personal data protection regime, in line with international standards, including as to any exceptions.
- The local data storage system in the draft Law should either be removed entirely or replaced with a far more narrow and tailored system that takes into account the needs of Internet service providers in Myanmar.
- The data retention requirements should be removed.
- The power of authorities to require Internet service providers to provide personal user data should be subject to appropriate legal conditions, in line with the purpose for which the authority is seeking access.

3. Content Restrictions

The draft Law contains a number of restrictions on the types of content that may be disseminated online, and puts in place systems to counter these types of content. The primary provision in this regard is section 29, calling for the "prevention, removal, destruction and cessation" by Internet service providers, "in a timely manner", at the request of the Department, of the types of content it identifies, where that content is "on cyber space". The exact modalities by which this system is intended to work are not clear from the provision. However, the approach appears to be very problematical. First, while all regulation by bodies that are not independent of government which affects freedom of expression represents a breach of international law, as noted above, direct content regulation along these lines by far the most problematical, for fairly obvious reasons (i.e. because such powers are likely to be used in a less than politically objective manner). Second, any system of content regulation should set out clear rules, including procedures, governing the way content deemed to be contrary to the rules will be addressed. This provision simply refers to a range of possible measures – prevention, removal, destruction, cessation – without indicating how the system will work. It seems likely that Internet service providers will simply be expected to do whatever the Department "orders" in relation to specific content. They may also be expected to take measures vis-à-vis the users responsible for this content, for example under the rubric of "prevention". If so, this provision would engage a number of due process and other rights concerns. Third, content regulation systems should incorporate due process protections for users, whereby they can contest any actions taken against their content. No such protection appears to be envisaged here. Fourth, the provision is unclear as to whether the content in question even needs to have been made available publicly. Cyber space includes fully public communications, such as open content on public websites, partially public communications, such as information shared with a pre-defined group on a social media platform, and private communications, such as one-to-one communications. All of these would appear to be captured by this provision.

Fifth, the specific types of content that are proscribed should align with what international law protections for freedom of expression allow. An initial point here is that it is not legitimate to duplicate in a cyber-specific law content restrictions which already exist in laws of general application. Otherwise, most of the specific categories of prohibited speech in section 29 do not meet the standards established by international law. Section 29(a) calls for the banning of "expressions causing hate, disrupting the unity, stabilisation and peace". At least the last three of these are far too vague and subjective to pass muster under international law as restrictions on freedom of expression. A minimum requirement here is that a prohibition must be sufficiently clear and precise to give advance warning to those who are subject to it to act in a way that avoids falling foul of the rules.

Section 29(b) covers "misinformation and disinformation". While superficially attractive, international law rules out generic bans on inaccurate information. There are various reasons for this, including the fact that everyone makes genuine mistakes and the often subjective nature of evaluating the accuracy of a statement. At the same time, international law does allow for bans on false information in specific circumstances, such as where it harms reputation (defamation law) or is present in sworn testimony before a court (perjury). No such condition is present in section 29(b). This provision is supplemented by section 64, which provides for up to three years' imprisonment and/or a fine for anyone who creates misinformation or disinformation with the intent of "causing public panic, loss of trust or social division". While this does include an intent requirement and link the crime of sharing inaccurate information to a result, that result is far too broad to render this prohibition legitimate. For example, a report that 45 people had died of COVID 19 in Myanmar might technically be inaccurate, if only 40 people had died, and might cause either panic or a loss of trust (say in government), and yet it would clearly be illegitimate to sanction such a report. Section 65 is very similar, albeit applying to the creation of a fake account, website or web portal, whatever fake might mean in this context.

Section 29(e) is perhaps the most problematical of the section 29 sub-sections, covering any "written and verbal statement against any existing law". This is simply not legitimate; the criticising of existing laws is not only a protected exercise of the right to freedom of expression but a key activity in any democracy which seeks to improve itself. It may be noted that were this Analysis about an existing as opposed to draft law, this provision would serve as grounds for blocking access to it.

Section 68 provides for imprisonment, again for up to three years, and/or a fine, for sharing or disseminating "sexually explicit speech". Whereas as the counterpart of this in section 29(c) is linked to Myanmar's cultural norms, this is significantly wider, covering anything that is sexually explicit even if it falls within the range of accepted cultural communication. Furthermore, while section 29 is unclear as to its scope, the language here suggests that even private communications, say between married people, would be covered. On the other hand, Section 69, which covers child pornography, is appropriate in its scope.

The problems with the provisions in sections 64, 65 and 68 are compounded by section 85, which provides that all of the offences in the draft Law are cognisable, meaning that the police

can arrest a suspect without a warrant and initiate an investigation without court authorisation. This category is normally reserved for more serious offences. While some of the offences envisaged in these provisions, for example relating to child pornography, are indeed very serious, others are not. Some minimum standard should be established before an offence is able to be treated as cognisable.

Recommendations:

- Section 29 should be removed in its entirety from the law. If any provision along these lines is retained, it should cover only content which international law allows restricting and which is unique to the online context so as to justify such a special online restriction.
- Sections 64, 65 and 68 should also be removed.
- Section 85 should either be removed entirely or amended so that only more serious crimes are classified as cognisable.

4. Other Criminal Rules

A large number of provisions in the draft Law create offences for various forms of online behaviour, a lot of which falls under the generic description of hacking although a number of other forms of behaviour are also covered. It is beyond the scope of this Analysis to analyse each of these provisions in detail. However, a few general comments are in order.

First, there is a tremendous amount of overlap among these provisions. For example, sections 36, 37, 38, 40, 41, 59 and 60 all deal with broadly similar offences (mostly relating to different forms of hacking). It is not clear what the structural distinction is between provisions in Chapter 11 (which contains sections 36, 37, 38, 40 and 41 from among those mentioned above) and Chapter 15 (which contains sections 59 and 60). The latter have specific penalties attached to them but otherwise overlap broadly with the former. Apart from this form of duplication, especially in different chapters of the draft Law, just being poor legal drafting and style, a number of problems may arise from it. It could create confusion for both those tasked with applying the law and those subject to it, leading to misapplications of the law or applications in ways that were not intended. Those responsible for applying the law may seek to interpret it in ways that differentiate the various provisions, so as to give them each a separate meaning, which could result in overextension of the law. Different provisions may be applied to the same sort of behaviour but lead to different results, given the slight differences in wording, resulting in injustice.

Second, given the nature of online behaviour, innocent but innovative or exploratory behaviour can lead to results that look like hacking or other forms of wrongdoing, for example where a programmer stumbles into an unauthorised space. As a result, clear and specific intent

requirements are very important to ensure that the rules are only applied to genuinely bad faith behaviour. Such intent requirements need to go beyond simple intent (i.e. an intention to do the act described) and should incorporate a more specific intent (such as bad faith or fraud or a desire to effect some other type of malfeasance). Section 62 is the first one which makes any specific mention of intent, in that case of "bad faith or dishonesty". The lack of any intent requirement in the other provisions may lead to them being applied too broadly.

Third, many of the provisions are phrased too broadly. For example, section 60 applies whenever someone discloses data to a third party without the consent of both the original sender and receiver. Almost everyone in the world who uses a digital device is guilty of this offence, which would be committed whenever someone who was copied on an email forwarded it to another person, without first getting the consent of the sender and the primary addressee. Section 39 does not even require any lack of authorisation, so that one may fall foul of it even using ones' own computer. Although section 62 does include an appropriate intent requirement, some of its rules are too broad, such as the prohibition on deceiving others.

In some cases, this overbreadth applies to the issue of intent. For example, section 70 refers to intent to hurt someone or threaten security (legitimate) but also to disturb national solidarity (not legitimate). Similarly, section 71 includes among its list of prohibited intents that of helping another country, which is normally perfectly legitimate.

Section 55 prohibits online gambolling without permission, but fails to specify who should provide such permission. This is buttressed by section 75, which provides that those who breach this rule shall be punished under the Gambling Law. It is possible that the latter indicates who may provide permission for gambolling and how one may obtain it. Otherwise, however, this sort of prohibition is likely to create confusion and potentially misapplication of the law.

Overall, these provisions should be rationalised and simplified – the legitimate goals they collectively cover could be captured in far fewer provisions – and the problems above should be addressed.

Recommendations:

- The various prohibitions on different sorts of online behaviour in the draft Law should be substantially revised and rationalised to remove duplication and similar offences being described with only minor, unclear linguistic difference. This applies with particular force to the rules in sections 36, 37, 38, 40, 41, 59 and 60, where the problem is particularly problematical given that these sections fall into two very different chapters of the draft Law.
- All of these prohibitions should be accompanied by clear and specific intent requirements which go beyond merely the intent to commit the act and include an intent to cause harm, act in bad faith or something else along those lines.
- Any prohibitions along these lines should be drafted in clear and narrow terms so that

they cannot be applied to innocent behaviours. This applies to both the main form of prohibited behaviour and the accompanying intent.
- The prohibitions on gambolling in sections 55 and 75 should be reviewed to ensure that they do not introduce an ambiguous reference to the idea of permission to conduct gambolling.

5. Burdens on Private Sector Actors

The draft Law places a number of burdens on private sector actors, mostly generally on Internet service providers but sometimes more specific rules for different sub-sets of that broad category. These have implications for freedom of expression inasmuch as many of these private actors serve to facilitate online speech such that undermining their ability to operate effectively or provide certain types of services has a knock-on effect for the freedom of expression of their users.

Section 27 applies to "cyber security service providers", defined quite broadly in section 3(v) as anyone who provides cyber security services either online or through technological systems or materials. These providers are all required to develop cyber security measures to support the Department and "Cyber Security Breach Emergency Response teams", provide warnings and "preventive guidance" on cyber security risks and develop "response plans and solutions" vis-à-vis various risks. The provision of cyber security services can take many different forms, ranging from the development of specialised software in different areas, the provision of training, the direct provision of technical support to clients and so on. Imposing these broad, uniform obligations on all of these actors is simply not appropriate. For example, a specialised software developer may not be in a position to provide solutions to hacking, as required by section 27(c).

According to section 44, Internet service providers, including cyber security service providers, must "coordinate and collaborate" with the three mandated Working Committees (on cyber security, cybercrime and cyber protection) in the areas set out in section 43. These include, as noted above, activities such as preventing further consequences of threats, attacks and other risks, preventing these risks from happening at all, increase levels of cyber security vis-à-vis information and investigating threats and attacks. Once again, the imposition of these uniform obligations on all Internet service providers is simply not appropriate. Indeed, it may be questioned whether it is appropriate to impose any of the obligations in sections 27 and 44 on private companies. Rather, this is an area where either the market should respond to needs or the public sector should manage affairs.

According to section 28(b), all Internet service providers must register in accordance with Myanmar company law. This would pose a serious barrier to any such companies which have limited business in Myanmar and which may nevertheless be providing important services to a small clientele in the country. It is also likely that many service providers based abroad would simply refuse to register locally, which would incur costs and render them subject to local

jurisdictional rules (note that if they did this in Myanmar, they could hardly refuse to do it in other countries as well). It is not clear how such a rule could be enforced in any case. A similar problem relates to section 28(c), about paying local taxes. While this may appear reasonable, and many jurisdictions are indeed looking at how they can claim taxes relating to profits which online companies in fact harvest in their countries, even if they do not have any material base of operations there, in fact the issue is quite complicated and a simple provision like this, which does not take into account any of the actual complexity of the situation, may put users at risk without actually being able to be implemented.

Sections 32-35 deal with licensing and registration, which is undertaken by the Department, while section 78 gives existing providers a year to renew their operating arrangements in this regard. While it is not unreasonable to expect, respectively, electronic certification issuers (section 32) and cyber security services (section 33) to have licences, given the security nature of their work, and Internet service providers to register (section 34), there are a few problems with this. First, there is the problem noted above, of companies that provide these services but are based in other countries. Second, it is not reasonable to require Internet service providers both to incorporate under the companies law and to register with the Department. Third, section 78 may breach the legal rights of some existing providers, potentially even through the Department refusing to renew a licence which had had a number of years' duration remaining. It is not clear why existing licences should not be continued, perhaps by providing that they are deemed to be amended as necessary to conform to the new legal rules. Finally, the importance of having this sort of function undertaken by an independent body has already been noted.

The problems with the provisions above are exacerbated by section 61, which provides for imprisonment for up to three years and/or a fine of up to MMK 10,000,000 (approximately USD 7,000) for breach by any Internet service provider of "provisions prescribed in this law". This is quite a harsh maximum penalty, especially for some of the rules. It is not clear how imprisonment might apply under Myanmar law to a company, which these entities would be legally required by the draft Law to be, but to the extent that directors might be personally liable under these provisions, this could deter worthy people from taking up these sorts of positions.

Recommendations:

- Consideration should be given to removing entirely sections 27 and 44. At a minimum, they should be scaled back considerably to apply only as appropriate and relevant to different Internet service providers.
- The rules on incorporation, taxation, licensing and registration should be fundamentally reconsidered. At a minimum, the working needs and reality of companies based abroad should be recognised and any obligations on them should be carefully tailored based on this, existing companies should have their licences respected and the sanctions should be more carefully adapted to the different sorts of breaches by private companies.

6. Critical Information Infrastructure

Chapter 7 of the draft Law deals with critical information infrastructure. This is defined in section 3(l) as "fundamental information infrastructures" but the definition then goes on to refer to a wide range of areas of public life such as public welfare, health and finance. Section 16 expands this even further to cover natural resources, communication and even infrastructure "classified for private use only", among other tings. For the most part, this chapter places various obligations on different actors to secure critical information infrastructure. While these obligations sometimes appear excessive given the breadth of the areas covered by this concept, that does not necessarily raise human rights issues.

However, section 20 addresses information security for critical information infrastructure, requiring officials responsible for this, among other things, to keep "information on" critical information infrastructure "at a place permitted by the Ministry" and to follow the rules in dealing with this information (it is not clear who sets those rules). Failure to meet these obligations may, pursuant to section 58, lead to imprisonment for up to three years and/or a fine. The exact scope of these obligations is not clear but it could potentially cover all the information held by all of the public authorities that work in all of these sectors. If so, this would represent a massive extension of essentially security-driven control over an enormous wealth of information which has nothing whatsoever to do with security. While this may appear to be a dramatic interpretation of these provisions, it is not out of line with some other legislation adopted recently by Myanmar relating to information.

Recommendations:

- The scope of the section 20 obligations should be limited to information the protection of which is essential to guaranteeing the ability of critical information infrastructure authorities to operate safely and free from cyber attacks, rather than all of the information they hold.
- Consideration should also be given to narrowing substantially the scope of authorities which are deemed to fall within the scope of critical information infrastructure.