Sector Wide Impact Assessment

Myanmar ICT Sector-Wide Impact Assessment

September 2015

Institute for Human Rights and Business

Myanmar Centre for Responsible Business

THE DANISH INSTITUTE FOR HUMAN RIGHTS

The Myanmar Centre for Responsible Business (MCRB) was set up in 2013 by the Institute for Human Rights and Business (IHRB) and the Danish Institute for Human Rights (DIHR) with funding from several donor governments. Based in Yangon, it aims to provide a trusted and impartial platform for the creation of knowledge, capacity, and dialogue amongst businesses, civil society organisations and governments to encourage responsible business conduct throughout Myanmar. Responsible business means business conduct that works for the long-term interests of Myanmar and its people, based on responsible social and environmental performance within the context of international standards.

Published by MCRB, IHRB and DIHR – September 2015.

Myanmar Centre for Responsible Business
15 Shan Yeiktha Street
Sanchaung, Yangon,
Myanmar
Email: info@myanmar-responsiblebusiness.org
Web: www.myanmar-responsiblebusiness.org
or www.mcrb.org.mm

Institute for Human Rights and Business (IHRB)
34b York Way
London, N1 9AB
United Kingdom
Email: info@ihrb.org
Web: www.ihrb.org

Danish Institute for Human Rights (DIHR)
Wilders Plads 8K
1403 Copenhagen K
Email:
info@humanrights.dk
Web:
www.humanrights.dk

Contents

Acknowledgements

The partner organisations would like to thank the Governments of Denmark, Ireland, Netherlands, Norway, Switzerland and United Kingdom for their on-going support to MCRB.

The partner organisations would also like to thank all those who participated in the field assessments across Myanmar, and in the June 2015 Yangon and London consultations on the draft ICT SWIA. They also thank the Union Government, as well as the Governments of Mandalay Region, Sagaing Region, Yangon Region, Shan State, Mon State and Kayin State, for their support in the research phase.

The report was written by: Margaret Wachenfeld, Donna Guest, Haley St. Dennis and Lucy Purdon of IHRB, Vicky Bowman, Kamran Emad, Thi Thi Thein of MCRB, with important contributions from Elin Wrzoncki and Rikke Frank Joergensen of DIHR.

The team would also like to recognise the contributions of the MCRB ICT field team: Research Leader Kamran Emad, SWIA Manager Thi Thi Thein and researchers: Sandar Cho Oo, Hlaing Min Oo and Kyaw Thura.

Special thanks go to Susan Morgan, who authored the Annex to the Recommendations on Lawful Interception and Government Access to User Data, with input from Lucy Purdon and Margaret Wachenfeld, and we would also like to thank all those experts interviewed for this section of the SWIA. We would also like to thank Asia Law & Justice Fellow Joey Lee of Fordham Law School and students Alison Cullen, Matthew Solomon and Jennifer Whitman who provided detailed research on ICT laws in Myanmar. The research also draws on background papers developed for MCRB by Kamran Emad, Delphia Lim and Ross Wilson as well as Dr Richard Horsey of Peace Nexus.

TERMS

Amyotha Hluttaw: The "House of Nationalities", which is the Upper House of the National Legislature and has 224 representatives – 168 are elected in equal numbers from each Region and State, i.e. 12 representatives from each Region or State. The 12 must include one elected representative from each Self-Administered Division or each Self-Administered Zone. 56 representatives are nominated by the Commander-in-Chief of the Defence Services, including 4 representatives from each Region or State. (Constitution of the Republic of the Union of Myanmar (2008), Article 141)
Constitution: The 2008 Constitution of the Republic of the Union of Myanmar which came into operation on the day the first session of the Pyidaungsu Hluttaw was convened (31 January 2011).
Hluttaw: A Burmese equivalent of "legislature." Myanmar has a National (Union) Hluttaw, and Hluttaws in each State and Region.
Pyidaungsu Hluttaw: The National (Union) Legislature, which is bicameral and composed of the Amyotha Hluttaw and the Pyithu Hluttaw.
Pyithu Hluttaw: The "House of Representatives" or the "People's Assembly", which is the Lower House of the National Legislature and has 440 representatives. 330 representatives are elected from township-based constituencies. 110 representatives are nominated by the Commander-in-Chief of the Defence Services. (Constitution, Article 109)
Tatmadaw: The Tatmadaw refers to the armed forces of the Union of Myanmar. The main armed force is the Defence Services, and all armed forces in the Union are under the command of the Defence Services. (Constitution, Articles 337 and 338)
Union/Myanmar Government: The Union Government comprises the President, the two Vice-Presidents, the Ministers of the Union, and the Attorney-General of the Union. (Constitution, Article 200)

ABBREVIATIONS

ADB	Asian Development Bank
ASEAN	Association of South-East Asian Nations
DICA	Directorate of Investment and Company Administration
CESD	Centre for Economic and Social Development
EHS	Environmental Health and Safety
ESIA	Environmental and Social Impact Assessment
FESR	Framework for Economic and Social Reforms
FPIC	Free, Prior and Informed Consent
GDP	Gross Domestic Product
GeSI	Global e-Sustainability Initiative
GNI	Global Network Initiative
ICCPR	International Covenant on Civil and Political Rights
ICT	Information and Communication Technologies
IFC	International Finance Corporation
IFI	International Financial Institution
MCRC	Myanmar Communications Regulatory Commission
MCIT	Ministry of Communications and Information Technology
MDRI	Myanmar Development Resource Institute
MIC	Myanmar Investment Commission
MIDO	Myanmar ICT Development Organisation

MMCERT	Myanmar Cybersecurity Emergency Response Team
MNPED	Ministry for National Planning and Economic Development
MOST	Ministry of Science and Technology
MPT	Myanma Posts and Telecommunications
NLD	National League for Democracy
OECD	Organisation for Economic Cooperation and Development
OHCHR	Office of the High Comissioner for Human Rights
PTD	Posts and Telecommunications Department
SLORC	State Law and Order Restoration Council
SPDC	State Peace and Development Council
SWIA	Sector-Wide Impact Assessment
UNDP	United Nations Development Programme
USDP	Union Solidarity Development Party
VOIP	Voice over Internet Protocol

LIST OF TABLES

LIST OF FIGURES

Executive Summary & Recommendations

EXECUTIVE SUMMARY

The roll-out of new information and communications technologies (ICT), infrastructure and services in Myanmar is having a transformative impact on the country. Mobile phone penetration has increased from 7% to 33% between 2012 and 2014, and continues to rise. The growing availability of smartphones is increasing opportunities for Internet access. It has been estimated that by 2030 the ICT sector could contribute $6.4 billion to Myanmar's GDP and employ approximately 240,000 people.

The ICT sector is having a transformative impact on Myanmar at the same time as the country itself is undergoing a transformation: emerging from decades of ethnic-based armed conflict, authoritarian rule and economic isolation. Myanmar is – and will remain for some time – a high-risk country with poor governance. The headlong rush to improve access to ICTs brings challenges, particularly in the absence of adequate policy and legal frameworks. These frameworks are lacking both for the rollout of the network and other services, and for considering and controlling wider impacts on society associated with greater use of ICTs, such as surveillance of communications and "hate speech" online. The gaps in the policy and legal frameworks are compounded by people's basic lack of experience of using ICTs, resulting in the potential for misuse and negative impacts on a range of human rights, particularly the rights to privacy and freedom of expression.

This means that conducting business responsibly in Myanmar's ICT sector requires a clear commitment to understanding the complex operating context and its constraints to determine what impacts business activities may have on people in Myanmar. This needs active engagement by companies, Government and civil society to promote public and informed debates, which are still a rarity in Myanmar. This also includes the need for robust approaches to filling in the gaps by managing negative impacts in line with international standards on responsible business conduct.

This Sector Wide Impact Assessment (SWIA) carried out by the Myanmar Centre for Responsible Business (MCRB), in partnership with its co-founders, the Institute of Human Rights and Business (IHRB) and the Danish Institute of Human Rights (DIHR) is focused on Myanmar's ICT sector. It is based on both desk-based and field research in Mandalay, Sagaing and Yangon Regions, and Shan, Mon and Kayin States. It includes in-depth analysis of existing Myanmar policy and legal frameworks relevant to the sector, as well as the historical, political and economic context. It also includes research on the policies and practices of a wide range of companies in the ICT sector in Myanmar in order to further understanding and set out an analysis of the sector and its actual and potential impacts on Myanmar society.

The idea behind a SWIA is to present key human rights risks and opportunities for the Government of Myanmar, companies operating in the sector, and civil society in order to improve the regulation and operations of the sector in a manner that provides benefit to

Myanmar, its people, and businesses. It is a forward-looking assessment that aims to contribute to preventing and minimising the sector's negative impacts as well as strengthening and improving the sector's positive impacts (See Chapter 1 for more detailed information on the purpose and methodology behind the SWIA).

Key Actors in the ICT Sector

Government of Myanmar

As with other sectors in Myanmar, the Government departments overseeing the ICT sector are reliant on a small group of overworked civil servants. Few have the technical capacity to pursue the Government's ambitious "e-agenda" of providing citizens with access to technology to help Myanmar accelerate its development and move from isolation to global connectivity and competition. The challenges of developing the sector are enormous – from planning the expansion of network infrastructure and services, to establishing appropriate technical standards for emerging platforms, to reinvigorating an education system for the 21st century. The ICT sector is innately interconnected, bringing with it a host of challenges in addressing international standards and international relations that are inherently foreign to a formerly long-isolated country. Development partners such as the World Bank and Asian Development Bank are, however, supporting with technical assistance, as demonstrated by the transparent process for awarding the telecoms licences in 2013.

Yet technical assistance is no substitute for Myanmar Government staff grappling with the day-to-day challenges themselves. This includes a legal framework that is not designed for the modern technological age, nor aligned with international standards that were of little interest to earlier military governments. The legacy from that era that is enshrined in laws intended to restrict communication and sits uneasily with a burgeoning sector that exists, in many ways, to do the opposite. The challenge of updating the policy and legal frameworks to keep pace with technological developments and stay in line with the Government's ambitious reform programme is matched by the far less visible, but no less significant, challenge of reorienting both the authorities' and people's mindsets towards governance based on openness, transparency and accountability. This SWIA seeks to highlight the significant gaps in policy and laws that should be addressed as part of the Government's policy and legal reform process.

Companies in the ICT Sector

As in other countries, there is great variability amongst the companies in the sector, from local start-ups to large multinationals. Unlike tech start-ups in other countries, small local companies have not often been exposed to key global debates in the sector, nor access to content in their own languages. The learning curve is therefore likely to be steep, not only in meeting expectations of international business partners, but also in understanding the need for and approach to key issues like protection of data and, importantly, international standards on responsible business.

The rush to expand the network means that many companies and their local subcontractors are learning on the job. Some bring with them established governance, health, safety, environment and labour compliance frameworks and monitor them with spot checks, while others do not operate any systematic safety procedures. The human rights impacts observed during the research were in some cases quite visible, particularly in tower construction and laying fiber, including safety violations and in some cases extremely poor working conditions. The short-term employment opportunities for unskilled workers and semi-skilled workers provide much sought after jobs. However, they are often temporary, and sometimes involve harsh working conditions and piecemeal pay. In the longer term, the sector offers many job opportunities, but the skills and capacity needs to be built among the workers required to fill them.

The competitive forces driving the market, such as the rush to rollout mobile phone networks, can also counteract the incentives that exist to apply responsible business standards in Myanmar. Research for this SWIA started in July 2014, when the operators were rolling out and launching their new networks under severe time pressure. However, some of the larger operators have their own standards of conduct, which can drive responsible business practice more widely in the sector, if they are willing and able to apply them robustly in such challenging circumstances. Lessons learned from international initiatives that address some key challenges in respecting human rights in the ICT sector can also be useful for Myanmar. This SWIA aims to highlight the risks, and capture some of those demonstration effects and lessons learned across a range of topics relevant to the operation of the sector.

Civil Society

The research also showed that very few civil society groups, human rights defenders or media organisations had an understanding of the sometimes complicated and technical human rights issues associated with the ICT sector. The SWIA is also intended to raise wider awareness among these groups.

Users and Communities

The research also revealed a hunger and enthusiasm for mobile phone connectivity and Internet access, with a rapid uptake of social media services in particular. But it also revealed little user awareness of either the risks that the ICT sector can bring to them or the wider opportunities for the country. Digital literacy is extremely low in Myanmar. This is compounded by the novelty of the concept of privacy as understood in international laws and standards. In a country with a limited concept of physical privacy, promoting the concept of digital privacy and data protection among users is critical.

As with other SWIAs carried out by MCRB, IHRB and DIHR, observable company engagement and two-way communication with communities and workers was lacking, particularly in association with the network roll-out. This is particularly important in ethnic minority areas, including those affected by conflict, where it is essential to take the time to engage directly with as wide a range of stakeholders as possible. It addition to building a more complete picture of the conflict and inter-communal dynamics, it enables companies to understand what concerns or questions local people may have about the introduction of

ICTs. The potential for the on-going conflicts in certain ethnic areas to block, delay or sabotage further roll out could lead to a deepening of the digital divide, reinforcing inequality in conflict areas unable to access and benefit from ICTs.

Five Main Themes Emerge from the ICT SWIA

- **Gaps in the policy, legal and regulatory framework:** Modern laws do not exist for most of human rights risks posed by the ICT sector in Myanmar, and in particular lawful interception, data privacy, access to information, certification bodies, cybersecurity, data protection and cybercrime. Myanmar needs to fill the regulatory gaps through a rights-based approach which learns from good (and bad) practice elsewhere.

- **Access:** There is an opportunity to create an investment climate that supports an extensive telecommunications network and strong competition to bring down prices and achieve universal access and accessibility of ICTs. It is important to include local languages and standardised Unicode fonts that allow full searchability and access to information. This will ensure that the whole country can enjoy the social and development benefits inherent in positive technological development and global connectivity.

- **Online "Digital Dangers":** With the benefits of greater access to modern technology and the Internet come certain risks and digital dangers. These include risks to data privacy, various forms of cybercrime, including child sexual abuse images and revenge porn, cyberbullying and stalking, and "hate speech". Other digital dangers include the wider consequences of Government-ordered mobile and Internet network shutdowns and the selective blocking of websites. Companies, Government and the media need to educate the public about these issues. They should highlight safe behaviours (such as encryption or not posting or emailing personal information) through Burmese and other local language communications including software and application agreements, media articles, and other channels.

- **"Offline" human rights issues:** Complex land laws and processes for granting land use to erect telecoms towers are just one of the many problems faced by the Government, communities, operators and their subcontractors regarding the national network rollout. Rapidly changing labour laws and low awareness of rights means workers, and in some cases employers, are not well informed about even the most basic labour rights protections. While that function is often filled by trade unions in other countries, in Myanmar independent unions are only just emerging after many years of prohibition and are therefore new to these issues. The forced labour previously associated with the last military government is now generally limited to conflict areas, but new forms of forced labour are emerging in the private sector. One such example found in the research were workers required to work for a businessman to pay off work-related debts. Corruption in the permitting process is also a risk around network rollout.

- **Exacerbating or addressing visible divisions in society**: ICT has the potential to be used to impact positively or negatively on the rights of groups at risk**,** such as children. While there are gradual improvements in some areas of discrimination, religious discrimination and related violence is a serious problem and in recent times

particularly impacting the Muslim community. The research and other reports have identified disturbing patterns of anti-Muslim “hate speech” on social media in particular. Yet ICTs also have the potential to improve the situation of some groups at risk, such as people living with disabilities, by providing them with services or income generation opportunities from which they were previously excluded. There are also more female than male graduates in ICT related study, opening potential new areas of employment for women.

Issues on the horizon

With little to no in-country manufacturing, and a desire for even the most basic, second-hand phones, problems seen in other countries with e-waste or environmental pollution have yet to emerge in Myanmar. They will doubtless do so in time. Due to the absence of manufacturing, the SWIA does not cover “conflict minerals” such as gold, tin, tungsten and tantalum, although the first three are all produced in Myanmar. Research on how these minerals are being produced and sold and their relation to on-going conflicts in the country would be a useful topic for further investigation.

Recs

Recommendations

These Recommendations build on the measures expected of governments and businesses under the UN Guiding Principles on Business and Human Rights. Governments have a duty to protect human rights and all businesses – Myanmar and foreign – in the ICT value chain have a responsibility to respect human rights. Key excerpts from the UN Guiding Principles are highlighted in boxes at relevant points below. Further global human rights guidance for the ICT sector is available from European Commission, "ICT Sector Guide on Implementing the UN Guiding Principles on Business and Human Rights" (2013).

Recommendations
To the Government of Myanmar

1. Establish a coherent policy framework for the ICT sector with adequate safeguards.

UN Guiding Principles on Business and Human Rights: The State Duty to Protect

1. States must protect against human rights abuse within their territory and/or jurisdiction by third parties, including business enterprises. This requires taking appropriate steps to prevent, investigate, punish and redress such abuse through effective policies, legislation, regulations and adjudication.

2. States should set out clearly the expectation that all business enterprises domiciled in their territory and/or jurisdiction respect human rights throughout their operations.

The Government has embraced the importance of providing citizens with open access to technology and has also committed to a "people-centred" approach to development. A balanced approach that stimulates the spread and uptake of ICTs services while protecting the rights and interests of the population will be required to realise the positive potential of the ICT sector for Myanmar society. (See Chapter 2 on ICT Government Institutions, Policies & Legal Frameworks for further information).

Key Points for Implementation

- **Include adequate human rights, environmental and social safeguards for private sector operations in the forthcoming Master Plans for the ICT Sector.** These include the ICT Master Plan, the E-Governance Master Plan, and the Telecommunications Master Plan. Suggested safeguards are highlighted at the end of each SWIA Chapter. In addition, each Masterplan should be underpinned by a commitment to **advancing government transparency, accountability and public participation**. As part of that commitment, the government should engage in open,

public and meaningful consultations on the Master Plans leaving sufficient time for stakeholders to comment. (See Chapter 2 on ICT Government Institutions, Policies & Legal Frameworks for further information).

- **Undertake ongoing identification, prevention and mitigation of the potential longer-term and cumulative human rights, environmental and social impacts** when developing new strategic directions for the ICT sector. This could apply to further development of ICT parks, increased manufacturing, or developing outsourcing services. The aim should be to avoid and reduce the potential longer-term and cumulative negative impacts. (See Chapter 5 on Cumulative Impacts for further information). The government should also consider and plan for the predictable **environmental impacts** of the sector, in particular **e-waste** generated by the disposal of ICT equipment.
- Complete the transformations at the Ministry of Communications and Information Technology (MCIT) to establish the Post & Telecommunications Department (PTD) as **an independent ICT regulator** and Myanmar Post and Telecommunication (MPT) as **a privatised telecommunications operator and Internet service provider (ISP).**

2. Improve ICT-specific legal and regulatory reforms to ensure appropriate safeguards around Government activities and a coherent framework for responsible business conduct in the ICT sector.

UN Guiding Principles on Business and Human Rights: State Regulatory and Policy Functions

3. In meeting their duty to protect, States should:

a) Enforce laws that are aimed at, or have the effect of, requiring business enterprises to respect human rights, and periodically to assess the adequacy of such laws and address any gaps;

b) Ensure that other laws and policies governing the creation and ongoing operation of business enterprises, such as corporate law, do not constrain but enable business respect for human rights;

c) Provide effective guidance to business enterprises on how to respect human rights throughout their operations;

d) Encourage, and where appropriate require, business enterprises to communicate how they address their human rights impacts.

UN Guiding Principles on Business and Human Rights: Ensuring Policy Coherence

8. States should ensure that governmental departments, agencies and other State-based institutions that shape business practices are aware of and observe the State's human rights obligations when fulfilling their respective mandates, including by providing them with relevant information, training and support.

Myanmar has embarked on an ambitious programme of legal and regulatory reforms across the board, including changes specifically focused on the ICT sector. An appropriate legal framework can protect the rights of the population and encourage responsible business conduct. (See Chapter 2 on ICT Government Institutions, Policies & Legal Frameworks for further information).

Key Points for Implementation

- Ensure forthcoming regulations under the *Telecommunications Law*, *Computer Science Development Law* and *Electronic Transactions Law* confirm that **criminal penalties cannot be applied for legitimate expression**.
- The regulations should also **clarify the procedures and safeguards for blocking or filtering content** in line with international human rights standards. Any takedown requests should target specific pieces of content, rather than access to whole domains.

Recs

- **Clarify and limit the *Telecommunications Law* provisions on telecommunications network shutdowns** in line with international standards**.** A suspension of telecommunication services (mobile and/or landline) must be prescribed by law and only invoked if there is a real and imminent threat to national security or a national emergency. There must be a clear and transparent process around who is authorised to make a shutdown request, it should be limited in geography, scope and duration, and should be publicly reported after the fact. Network shutdowns affecting the whole country should never be authorised.
- **Make a commitment not to shut down the network during the upcoming elections.** Instead put in place plans to deal with potential emergencies, such as appropriate restrictions on the circulation of mass messages inciting violence and hate speech.
- **Introduce regulations on protecting data privacy** in line with international standards.
- **Mandate clear data protection and security standards** for entities licensed to provide mobile money services and other online services.
- **Consider alternative options to mandatory SIM card registration** given the potential chilling effects on freedom of expression.
- **Do not prevent companies from reporting** on the nature and number of **requests they receive from the Government of Myanmar** for lawful interception, communications data, content removal or blocking of websites, or requests for network shutdowns.

3. Improve wider legislative and regulatory reforms on freedom of expression and association, land use and management and labour issues to ensure appropriate safeguards around Government activities and a coherent framework for responsible business conduct in the ICT sector.

There are a wider range of laws that affect the ICT sector and users in Myanmar, many of which are part of the Government's ambitious programme of legal and regulatory reforms. As with the ICT-specific laws, these reforms should encourage further ICT development but in a way that protects the rights of the population and encourages responsible business conduct. (See Chapter 2 on ICT Government Institutions, Policies & Legal Frameworks for further information).

Key Points for Implementation

Freedom of Expression and Association:

- **Amend the *Law Relating to Peaceful Assembly and Peaceful Procession* to eliminate the criminalisation of protests and demonstrations,** which are increasingly taking place using ICTs.
- **Amend key laws restricting the right to freedom of expression**, including *1908 Unlawful Associations Law*, *1950 Emergency Provisions Act*, *1923 Official Secrets Act*, and various articles of the *Penal Code*, especially *Article 505(b)*.
- **Fully implement *Articles 3* and *4* of the *2014 Media Law*,** which provide for **"freedom from censorship"** and freedom to criticise the Government. Ensure that the media, including online journalists, are able to perform their legitimate functions without fear of censorship or arrest.

See Chapter 4.1 on Freedom of Expression for further information.

Labour:

- **Develop a comprehensive and overarching labour law framework** in line with international labour standards. Extend protection to all types of workers, including temporary and migrant workers. Given the expected expansion of employment in the ICT sector, and the competition to retain skilled Myanmar nationals, reinforcing the Government's commitment to the ILO's programme on Decent Work will be an important signal to workers and to ICT sector employers.
- **Strengthen the protection of workers involved in trade union activities** to ensure that they do not face discrimination or dismissal by employers solely for their legitimate trade union activities. Support trade unions to operate at the sector level so that they can adequately represent workers, including in growing sectors such as ICT where an increasing number of workers are expected to be employed. Raise awareness among employers with more than 30 workers about the legal requirement to put in place a workplace coordinating committee.
- **Demonstrate that the Government is committed to gender equality** by encouraging the employment of the large number of female graduates in ICT related studies, on the basis of equal pay for equal work.
- **Task labour inspectors with targeting their visits to high-risk sites,** such as tower construction and fibre trenches.

See Chapter 4.6 on Labour for further information.

Land Use and Management:

- **Ensure the forthcoming National Land Use Policy reflects the customary, informal and communal land ownership and use** arrangements in Myanmar, both in terms of protecting security of tenure and ethnic minority rights.
- **Establish a coherent legal framework for land use in line with international standards** (such as the FAO Voluntary Guidelines on the Responsible Governance of Tenure of Land, Fisheries and Forests in the Context of National Food Security) for private sector operations within the forthcoming comprehensive land law. This should ensure the protection of existing use and ownership rights while providing certainty and clarity around permitted transactions. This includes reforming existing land dispute mechanisms to enable enforcement of resolutions relating to land.
- **Clarify and simplify land classification and use procedures** to provide appropriate protection for farmers from unscrupulous land transactions and for food security. These should be sufficiently flexible to allow farmers to pursue alternative livelihood options on a portion of their land (such as leasing it for telecom equipment) and/or encourage local entrepreneurship.
- **Encourage telecommunications operators to follow the World Bank's** Myanmar Telecommunications Environmental and Social Management Framework and Land Lease Guidelines, including requiring their subcontractors to follow these guidelines in all land dealings.
- **Promote the sharing of tower infrastructure** to limit the impact on land take and improve efficiency.

See Chapter 4.7 on Land for further information.

Groups at Risk:

- Develop a more comprehensive framework for **child protection**, including relevant provisions for child safety online. The Government should consider asking companies and other governments to share expertise and good practices from other jurisdictions.
- Consider including **protections for women against online harassment** in the forthcoming law on violence against women.

See Chapter 4.8 on Groups at Risk for further information.

4. Adopt a rights-respecting lawful interception model and maintain open access to the Internet to ensure Myanmar does not become a modern "surveillance state".

UN Guiding Principles on Business and Human Rights: The State-Business Nexus
5. States should exercise adequate oversight in order to meet their international human rights obligations when they contract with, or legislate for, business enterprises to provide services that may impact upon the enjoyment of human rights. *6. States should promote respect for human rights by business enterprises with which they conduct commercial transactions.*

The Government has previously used ICTs to conduct surveillance of its citizens, both within the country and abroad. A modern legal framework limiting Government surveillance is overdue. (See Chapter 4.4 on Surveillance for further information).

Key Points for Implementation

- Follow through on the Government's stated commitment to **align the forthcoming lawful interception regulations or framework to international human rights standards.** See the **Annex to the Recommendations** for key considerations for each step of the interception process that should be incorporated into the forthcoming regulations. As it has with other draft ICT laws and regulations, MCIT should make any draft regulation or framework on lawful interception available for public comment for at least three weeks, and widely publicise the consultation process.
- **Publicly commit to prohibit "mass surveillance**" (commonly understood to refer to the bulk access and/or collection of many users' communications without prior suspicion of criminal activity). Such a commitment should also be incorporated into the forthcoming lawful interception regulation or framework (which should authorise only targeted interception where there is a prior suspicion of recognisably criminal activity).
- **Refrain from purchasing and utilising invasive and often unregulated communications surveillance technology** to carry out communications surveillance. Once Myanmar intelligence agencies have such capabilities, it will be much more difficult to eliminate or regulate their use. It is important for the Government, and the ICT companies that may be subject to lawful intercept orders, to make the distinction between software and other tools that comply with international standards on lawful interception, and products that fall below international standards because they are unregulated and pose a risk to human rights.

5. Improve data protection standards and cybersecurity.

Myanmar currently does not have any requirements or standards on data protection for companies. A failure to protect people's personal information and identity can pose significant risks to the right to privacy and security. As Myanmar puts in place its

cybersecurity infrastructure, and the laws and regulations underpinning it, it will be important to balance the legitimate need to combat cybercrime with human rights protections. (See Chapter 4.5 on Cybersecurity for further information).

Key Points for Implementation

- **Establish clear standards of data protection for companies and other organisations collecting, storing, or sharing user data.** This includes standards around data privacy, requirements to make privacy policies publically available, prior informed consent for the use of data and grievance mechanisms for users, and baseline security standards.
- **Promote awareness of the importance of cyber security for users** and build digital literacy through clear and concise communication. Widely disseminate basic best practices for users in partnership with the **Myanmar Computer Emergency Response Team (MMCERT).**
- **Do not criminalise the use of encryption tools by individuals**. Encryption is essential, not just for security of transactions but also the safety of human rights defenders. Blanket prohibitions on encryption, and therefore anonymity of communications, are not a necessary and proportionate response in line with international human rights standards.
- **Consider establishing a National Data Protection Authority** that would be in charge of the protection of data and privacy and that can handle complaints from users.

6. Demonstrate a commitment to free and open communication through a modern Freedom of Information law and build meaningful transparency systems across Government.

The Government has made a welcome commitment to join the Open Government Partnership and to modernise its approach to governance through its e-Governance Master Plan. It will be important to embed protections around the right to privacy into e-governance approaches so that they are trusted and can become a driver for ICTs and innovation. (See Chapter 4.1 on Freedom of Expression for further information).

Key Points for Implementation

- **Adopt a modern Freedom of Information Act**, as part of other steps towards **transparency** (e.g. commitments to join the Open Government Partnership by 2016, candidacy for Extractives Industries Transparency Initiative, and conducting more transparent licensing processes). If the **Constitution** is to be amended, include constitutional guarantees of public access to information held by the Government.
- Ensure that **privacy/data protection requirements** and safeguards are embedded into e-governance and open data initiatives.
- **Commit to access to information requirements that are aligned with the Open Government Partnership Principles**: the publication of all government-held information (which is broader than information only on government activities); proactive and reactive releases of information; mechanisms to strengthen the right to information; and open access to government information.
- **Commit to implementing core open data principles**, including across on-going national e-governance projects, such as the Common Citizen Service Data Portal to be

developed by MCIT and the World Bank. Given the increasing prevalence of mobile phones, ensure Government data displays are user-friendly and mobile-friendly.

- **Consult publically with civil society and business to identify high-value data** that catalyses innovation, enhances social policy, and promotes public and private sector accountability.

7. Accelerate the implementation of Myanmar's universal service commitments.

Until recently, Myanmar was at the bottom of the global league table for Internet and mobile phone penetration. While penetration rates are increasing rapidly, it may take years to reach all of Myanmar's population, particularly in rural areas. The Government tentatively committed to a universal service agreement with the current telecommunications operators, which called for each operator to contribute 2% of annual revenue to a universal service fund managed by MCIT, beginning after three years of successfully meeting network rollout targets. Myanmar has also joined the Alliance for Affordable Internet (AFAI). All parties can play a role in accelerating the roll out of services using innovative solutions so that a wider percentage of the population benefits from accessing ICTs. (See Chapter 3 on Sector Impacts for further information).

Key Points for Implementation

- **Publically disclose the current national rollout requirements for operators,** compared with their current progress.
- Build on lessons learned in the World Bank supported programme of **extending connectivity to rural areas**.
- **Develop a Universal Service Strategy,** as a first step in the implementation of Chapter XV of the *2013 Telecommunications Law*. **Consult widely**, including with ethnic minorities and disadvantaged groups such as people with disabilities, to identify priority areas for the rollout of telecommunications service (both mobile and fixed line broadband service), for inclusion in the Universal Service Strategy and Fund.
- Clarify how the Universal Service Fund will support **Myanmar's commitment to the Alliance for Affordable Internet,** which is focused on realising entry-level broadband priced at less than 5% of monthly income, particularly in rural communities
- **Consider allocating Universal Service Funds to support community-based telecommunications networks** and provide wireless spectrum concessions to remote rural communities where telecommunications service is currently inaccessible. This will help promote the development of low-cost community-based telecommunications networks for last mile or last inch connectivity.

8. Improve digital literacy of users and send clear signals about respectful use of ICT's.

To realise the range of transformative positive impacts via ICT growth and development in Myanmar, the Government must ensure that all Myanmar's population can participate in Myanmar's growing information society. Those services must be used respectfully so that violence and discrimination happening offline are not magnified and intensified online. This requires strong signals from opinion-formers, including Government. Engagement with ICTs is still a completely new experience for the majority of Myanmar people*. There is also a need for efforts from Government, business and civil society to provide*

awareness and training on protection against threats. (See Chapter 3 on Sector-level Impacts and Chapter 4.3 on Privacy for further information).

Key Points for Implementation

- **Ensure ICTs are "localised" for Myanmar users,** meaning technologies and content, including data and text, are adapted to support the wide range of languages in Myanmar, in addition to Burmese. The Government should commit to supporting the development of hardware, software, education materials, user manuals, amongst others, in all the main languages of Myanmar.
- **Support awareness raising campaigns and training around online safety and behaviour, including child safety**.
- **Send clear public signals from the highest level of government and all political parties that "hate speech" is unacceptable**. Hate speech spreads quickly online and has been used to incite violence. The Myanmar Government should actively support efforts aimed at "counter speech", where users challenge "hate speech" for example, by exposing false rumours, ideally with the support of the police, and encouraging peaceful expression.
- **Prioritise public education sector reforms that include a modernised ICT curricula for higher and vocational education** to meet the needs of employers.

9. Strengthen requirements for responsible business conduct in the ICT sector, including by requiring companies to provide operational grievance mechanisms for anyone impacted by their activities, and to report on their implementation.

UN Guiding Principles on Business and Human Rights: Access to Effective Remedy
25. As part of their duty to protect against business-related human rights abuse, States must take appropriate steps to ensure, through judicial, administrative, legislative or other appropriate means, that when such abuses occur within their territory and/or jurisdiction those affected have access to effective remedy.
UN Guiding Principles on Business and Human Rights: Operational Grievance Mechanisms
29. To make it possible for grievances to be addressed early and remediated directly, business enterprises should establish or participate in effective operational-level grievance mechanisms for individuals and communities who may be adversely impacted.
UN Guiding Principles on Business and Human Rights: Effectiveness criteria for non-judicial grievance mechanisms
31. In order to ensure their effectiveness, non-judicial grievance mechanisms, both State-based and non-State-based, should be: *(a) Legitimate: enabling trust from the stakeholder groups for whose use they are intended, and being accountable for the fair conduct of grievance processes;* *(b) Accessible: being known to all stakeholder groups for whose use they are intended, and providing adequate assistance for those who may face particular barriers to access;* *(c) Predictable: providing a clear and known procedure with an indicative time frame for each stage, and clarity on the types of process and outcome available and means of monitoring implementation;* *(d) Equitable: seeking to ensure that aggrieved parties have reasonable access to sources of information, advice and expertise necessary to engage in a grievance process on fair, informed and respectful terms;* *(e) Transparent: keeping parties to a grievance informed about its progress, and providing sufficient information about the mechanism's performance to build confidence in its effectiveness and meet any public interest at stake;* *(f) Rights-compatible: ensuring that outcomes and remedies accord with internationally recognised human rights;* *(g) A source of continuous learning: drawing on relevant measures to identify lessons for improving the mechanism and preventing future grievances and harms;*

Recs

Operational-level mechanisms should also be:
(h) Based on engagement and dialogue: consulting the stakeholder groups for whose use they are intended on their design and performance, and focusing on dialogue as the means to address and resolve grievances.

The Government should clearly signal its expectations to companies (foreign or local) that it expects responsible investment aimed at the long-term interests of Myanmar and all of its people. That expectation can be expressed in policies and law (see the Recommendations to the Government of Myanmar, numbers 2 and 3, above). It can be strengthened through public awareness raising and capacity building of Myanmar companies, and by ensuring that they make themselves accountable to the population (see Recommendations to Companies below). As Myanmar's judicial system reforms will take many years, in the interim, it is important that effective alternatives to formal legal proceedings are available to ensure that access to remedy is readily available to those adversely impacted by business activities.

Key Points for Implementation

- **Set out the Government's expectation that businesses investing and doing business in Myanmar will engage in responsible business conduct,** whether through enterprise registration or through a permit from the Myanmar Investment Commission (MIC). This could for example be through public guidance from the Directorate of Investment and Companies Administration (DICA) to all Myanmar and foreign companies.
- **Include two contractual terms relating to responsible business in MIC Permits, requiring**:
  - An annual report explaining the company's approach and outcomes in conducting business responsibly
  - All companies granted a MIC permit should establish mechanisms to receive and constructively address concerns and complaints, from workers, communities and civil society, consistent with the effectiveness criteria of principle 31 of the UN Guiding Principles on Business and Human Rights

Recommendations
To ICT Companies

1. Apply international standards of responsible business conduct in the absence of developed national legal frameworks, in particular the UN Guiding Principles on Business and Human Rights.

UN Guiding Principles on Business and Human Rights: The Corporate Responsibility to Respect

10. Business enterprises should respect human rights. This means that they should avoid infringing on the human rights of others and should address adverse human rights impacts with which they are involved.

UN Guiding Principles on Business and Human Rights: Human Rights Policy Commitment

15. In order to meet their responsibility to respect human rights, business enterprises should have in place policies and processes appropriate to their size and circumstances, including:

- *a) A policy commitment to meet their responsibility to respect human rights;*
- *b) A human rights due diligence process to identify, prevent, mitigate and account for how they address their impacts on human rights;*
- *c) Processes to enable the remediation of any adverse human rights impacts they cause or to which they contribute.*

UN Guiding Principles on Business and Human Rights: Human Rights Due Diligence

17. In order to identify, prevent, mitigate and account for how they address their adverse human rights impacts, business enterprises should carry out human rights due diligence. The process should include assessing actual and potential human rights impacts, integrating and acting upon the findings, tracking responses, and communicating how impacts are addressed. Human rights due diligence:

- *a) Should cover adverse human rights impacts that the business enterprise may cause or contribute to through its own activities, or which may be directly linked to its operations, products or services by its business relationships;*
- *b) Will vary in complexity with the size of the business enterprise, the risk of severe human rights impacts, and the nature and context of its operations;*
- c) *Should be ongoing, recognising that the human rights risks may change over time as the business enterprise's operations and operating context evolve.*

This SWIA has highlighted the current gaps in the Myanmar's evolving policy and legal framework. Due to the rapid pace of change, and lack of capacity and experience among legislators and Government ministries, there is no guarantee that, once adopted, Myanmar laws will fully reflect international standards. Nor are they guaranteed to protect workers, users, communities and the businesses themselves from the risks highlighted in the SWIA. In addition to providing companies certainty at a time when the national legal landscape is in flux, using international standards – such as the UN Guiding Principles on Business and Human Rights (and the OECD Guidelines on Multinational Enterprises for the companies to which they are applicable) – also provides confidence to local and international stakeholders. Because the situation is changing so rapidly, ICT sector companies should consistently scan their operating environments to understand the human rights risks that may be created by Government actions, or by their own operations, or those of their business partners.

Recs

Key Points for Implementation

- **Adopt a policy commitment to respecting human rights**, and ensure it is embedded across the company and widely communicated to stakeholders. Such a public commitment is important because it demonstrates that top management consider respect for human rights as a minimum standard to conduct business with legitimacy. A few Myanmar companies have begun to adopt human rights commitments and publicly report on implementation.[1] Such commitments signal to local stakeholders a break with the past. To international business partners they signal an awareness of, and commitment to, operating in accordance with international standards.
  - **Ensure other operational policies and processes** are aligned with the human rights commitment, for example, **clear and accessible privacy policies** that explain the company's policy on protection and its use or sale of customer's data. For ICT companies that interact directly with users or customers, the company's **Terms of Service, "user community" guidelines or similar documents**, should explain the use of the company's services in clear and accessible language, including in Burmese and other local languages.
- **Carry out human rights due diligence on an on-going basis:**
  - **Assess the risks and impacts the company and the other companies in its value chain** (suppliers, contractors, etc) **could pose to people and their human rights**.
    - Take account of local complexities and legacies, including **the considerable gaps in the existing legal framework** identified in the Recommendations to the Myanmar Government, numbers 2 and 3 (and throughout this SWIA). Seek to fill those gaps by operating according to international standards. Take account of **conflict dynamics** when operating in areas of latent, existing and potential armed conflict.
    - **Explicitly consider** risks of contributing to or being directly linked to Government or business partners' actions that may violate human rights. This should go beyond simply ensuring that business partners are not, nor have been, on the US or other sanctions list. Given the past involvement of some businesses in government or military related human rights abuses, careful due diligence is necessary including around the company's commitment to responsible business practice, transparency and international standards.
  - Use the assessment of potential risks **to identify and implement steps to prevent or at least mitigate those risks.** The types of actions will vary considerably. It might include taking collective action to work with the Government to address gaps in the laws (see Recommendation 5 below), or specific actions in conflict-affected areas. See Recommendation 3 below on the wide range of risks and suggested responses highlighted in the SWIA.
  - **Track responses to identified risks and impacts**. Consider how workers, communities, users, customers and others potentially affected by company operations can be involved in monitoring activities.
  - **Communicate publicly about** what the company is doing to address the human rights impacts raised in this SWIA and more broadly, particularly when concerns

[1] Pwint Thit Sa/Transparency in Myanmar Enterprises Report (2015) is intended to encourage increased transparency by Myanmar businesses by rating them based on information they publish on the internet in the areas of anti-corruption, organisational transparency, and human rights, health, safety and the environment.

are raised by affected stakeholders, as recommended in MCRB's Pwint Thit Sa/TiME project.

- Proactively **report on the requests received from the Myanmar Government** (at all levels) for lawful interception, communications data, content removal and website blocking, and requests for network shutdowns, in order to stimulate further transparency around what the Government is asking companies to do and how companies are responding.
- **Make it easier for Myanmar users to communicate with the company** by providing services in local languages and offering services that come pre-loaded with Myanmar fonts.
- **Focus on simply and clearly communicating risks** to users (such as through graphic icons), including terms of service, privacy policy etc.

2. Incorporate the thematic risks and recommendations presented throughout this SWIA into company operations and interactions.

The Recommendations in this section reflect a set of cross-cutting and overarching actions to ensure responsible business conduct in Myanmar's ICT sector. In addition, each of the ten sections in Chapter 4 include specific thematic recommendations that provide more detailed considerations that companies should consider in their on-going human rights due diligence, operations and actions.

Key Points for Implementation

See the specific recommendations from Chapter 4:

- Chapter 4.1: **Freedom of Expression & Opinion** Recommendations for ICT Companies
- Chapter 4.2: **Hate Speech** Recommendations for ICT Companies
- Chapter 4.3: **Privacy** Recommendations for ICT Companies
- Chapter 4.4: **Surveillance** Recommendations for ICT Companies
- Chapter 4.5: **Cyber-Security** Recommendations for ICT Companies
- Chapter 4.6: **Labour** Recommendations for ICT Companies
- Chapter 4.7: **Land** Recommendations for ICT Companies
- Chapter 4.8: **Groups at Risk** Recommendations for ICT Companies
- Chapter 4.9: **Stakeholder Engagement & Grievance Mechanisms** Recommendations for ICT Companies
- Chapter 4.10: **Conflict & Security** Recommendations for ICT Companies

3. Engage with potentially affected stakeholders, particularly workers, communities, customers and users, to build trust and demonstrate transparency and accountability.

Engagement cuts across many recommendations concerning improved human rights practices by companies, and is integral to their success. Sincere, on-going two-way engagement with workers, workers' representatives, users and communities is one of the most valuable things a company can do to prevent and mitigate risk, particularly in the Myanmar context where there has historically been a lack of trust of companies by communities and others.

Key Points for Implementation

- **Proactively undertake ongoing and meaningful engagement** with workers, their representatives, users and communities throughout the project lifecycle, including at early stages of activities and key operational moments where risks change, recognising that engagement is a new concept for many in Myanmar. For example, Myanmar labour law requires an employer with more than 30 workers to form a Workplace Coordinating Committee (2 representatives of workers, 2 representatives of employer) whether or not there is labour organisation (e.g. union) in the enterprise. This kind of joint committee provides the outlet for mutually beneficial joint monitoring of working conditions by workers and the enterprise.
- **Provide basic information to users and customers about how to stay safe online** by protecting personal data, and support digital literacy growth for users, including the need to manage their "digital footprint" across devices and services and reporting concerns.
- **Proactively provide information in a variety of formats** and understandable local language(s) on key issues that are of concern to the Myanmar public, such as the health and safety impacts of mobile phones and cell towers.
- **Online consultation and communication is nascent in Myanmar**, but webchats could be a form of communication with stakeholders who are increasingly expecting to access responses from companies via their Facebook pages.

4. Put in place mechanisms that can address concerns and grievances quickly and effectively.

UN Guiding Principles on Business and Human Rights: Remedying Impacts
22. Where business enterprises identify that they have caused or contributed to adverse impacts, they should provide for or cooperate in their remediation through legitimate processes.
UN Guiding Principles on Business and Human Rights: Effectiveness Criteria
31. In order to ensure their effectiveness, non-judicial grievance mechanisms, both State-based and non-State-based, should be: *(a) Legitimate: enabling trust from the stakeholder groups for whose use they are intended, and being accountable for the fair conduct of grievance processes;* *(b) Accessible: being known to all stakeholder groups for whose use they are intended, and providing adequate assistance for those who may face particular barriers to access;* *(c) Predictable: providing a clear and known procedure with an indicative time frame for each stage, and clarity on the types of process and outcome available and means of monitoring implementation;* *(d) Equitable: seeking to ensure that aggrieved parties have reasonable access to sources of information, advice and expertise necessary to engage in a grievance process on fair, informed and respectful terms;* *(e) Transparent: keeping parties to a grievance informed about its progress, and providing sufficient information about the mechanism's performance to build confidence in its effectiveness and meet any public interest at stake;* *(f) Rights-compatible: ensuring that outcomes and remedies accord with internationally recognised human rights;* *(g) A source of continuous learning: drawing on relevant measures to identify lessons for improving the mechanism and preventing future grievances and harms;* *Operational-level mechanisms should also be:* *(h) Based on engagement and dialogue: consulting the stakeholder groups for whose use they are intended on their design and performance, and focusing on dialogue as the means to address and resolve grievances.*

There are few outlets in Myanmar for effective resolution of grievances either through judicial or non-judicial means. This makes company-based alternatives all the more important to ensure issues are identified early and addressed quickly before they

escalate. One of the most efficient ways for a company to remediate impacts is through an operational-level grievance mechanism that is directly accessible to individuals, users and communities who may be adversely affected by the business and which can act as an early warning system about concerns. As with other dimensions of the corporate responsibility to respect human rights, the expectation that companies provide a remedy for harm they are involved in applies to all companies, foreign and Myanmar. Some of the larger Myanmar based companies are just beginning to address the need for establishing grievance mechanisms for workers, communities and civil society[2] as are some of the international companies operating in Myanmar.[3]

Key Points for Implementation

- **Set up an accessible and local information point** for all issues concerning larger projects, and in particular network infrastructure. This could start with actions as simple as putting contact phone numbers on infrastructure if local villagers want to raise concerns about the equipment; it could also be a network of locally based liaison officers, or community volunteers, or a dedicated CSO with a two-way connection to the company.
- **For ISPs and "Over the Tops**": **Develop community standards** about the kind of content permitted on the site and mechanisms for users to report content they find disturbing (such as a "Report Concerns" button or link on the website). Undertake basic user awareness raising campaigns to ensure such mechanisms are known and effective.
- **Develop a mechanism (or mechanisms) that provides accessible and effective processes for users, workers or communities to address concerns directly** about a company or its business partners. Accessibility will need to be considered carefully in light of the services the company offers, local languages, availability of ICTs, or whether "toll free" services are available to call so that users do not have to pay.
- **Design any mechanism with worker and community input to be consistent with the effectiveness criteria** under the UN Guiding Principles on Business and Human Rights.[4] It should guarantee that there will be no retaliation against complainants inside and outside the company, and that complainants are free to choose whether to use the company's mechanism or opt for remediation processes by state or third-party institutions.

5. Take collective action where appropriate to address human rights, social and environmental issues.

There is a value to companies in the ICT sector coming together to approach sensitive topics collectively and sharing lessons learned on applying international standards, including from other comparable countries. Collective action by companies can be more effective, less labour intensive for Government, and reduce exposure for individual

2 MCRB's, Pwint Thit Sa/Transparency in Myanmar Enterprises surveys companies for whether they have operational grievance mechanisms. On 3 June 2015 MCRB held Workshop for Business on Operational Grievance Mechanisms.

[3] See for example, Phillips reports that it has developed a Myanmar specific grievance mechanism: http://business-humanrights.org/en/response-by-philips-myanmar-foreign-investment-tracking-project

[4] UN Guiding Principles on Business and Human Rights, Principle 31 (see Recommendation to Government No. 9).

companies. There are a number of areas where companies may find it relevant to act collectively in discussions with the Government and other stakeholders.

Key Points for Implementation

- Collectively engage with the Myanmar Government **on filling the gaps within ICT and cross-cutting laws** to ensure alignment with international standards (See Government Recommendations 2 and 3).
- Collectively approach the Government on **applying international human rights standards around peaceful protest**, which are increasingly taking place using ICTs.
- Promote **learning on human rights issues** between foreign and Myanmar companies through engagement and support the creation of a sector-wide ICT industry association that includes foreign and domestic companies to support a coherent and coordinated approach to collective engagement.
- Work with development partners to **adapt higher education and vocational training** programmes to build skills for the ICT sector, and programmes to support SMEs.
- Support the variety of efforts across the country to **promote peaceful freedom of expression**, to counter hate speech, and to eliminate hate speech on ICT's.

6. Develop strategies for creating positive impacts at the local, regional and national level.

Key Points for Implementation

- **Develop social investment programmes with, for and by communities and users** to ensure focused, "strategic CSR" and ensure engagement and transparency around such programmes, including an annual public report and budget.
- **Promote small business and entrepreneurship programmes** to improve the ability of local businesses to meet ICT operator and subcontractor needs.
- **Commit to providing ICTs that are accessible to the disabled** and **improve livelihoods for people living with disabilities** in the country, given the very low level of employment for people living with disabilities or even access to services.
- Work with the government and other stakeholders to **provide access to language localisation and conversion resources.**

Recommendations

To CSOs, Human Rights Defenders and Media

1. Actively advocate for and comment on changes to ICT policy, laws and regulations, particularly with regard to human rights impacts.

Myanmar is in the process of developing or revising significant parts of the policy framework (such as the Master Plans cited in Recommendation 1 to the Myanmar Government), the laws and important regulations (such as under the 2013 Telecommunications Act, see Recommendations to the Myanmar Government, numbers 2 and 3). The Government staff and consultants working on these areas will be technical experts but potentially unfamiliar with the impacts on human rights of their policy advice. The same is true of Parliamentarians considering draft legislation.

Active civil society participation in advocating for and commenting on such changes will be important in ensuring that the final policy, legal and regulatory structure is appropriately balanced to provide for an efficient and effective ICT sector that guarantees protection of data and privacy and contains appropriate human rights safeguards. This should not only engage the limited number of Myanmar CSOs with ICT expertise; CSOs representing other interest groups such as women, ethnic minorities, children and people with disabilities should ensure their views are represented in ICT policy and legislation, since all are actual or potential users of ICT.

2. Hold companies to account on responsible business conduct, including around human rights.

There is an active, global discussion worldwide on the responsibility to respect human rights by companies in the ICT sector.[5] Some of these discussions focus on company conduct and others focus on the increasingly complex interplay between companies and governments, in terms of the appropriate limits to government power to request or directly access private data held by companies. Some of the initiatives in the area are multi-stakeholder, with companies and civil society and sometimes also with government working on solutions together. Many of these resources have been cited throughout this SWIA (see the boxes on International Standards and Guidance, as well as Myanmar initiatives, at the end of each of Chapter 4 and Chapter 5). They provide guidance on what can be expected of companies in the ICT value chain that can be used by CSOs to engage in informed discussions with companies operating in Myanmar.

[5] See for example the Business and Human Rights Resources Centre website on information technology and developments concerning companies in the sector.

3. Encourage companies and government to engage in multi-stakeholder discussion on human rights, social and environmental issues within the ICT sector.

There are no existing multi-stakeholder initiatives in Myanmar that will bring together companies, government and civil society into a common framework for discussion on ICT issues. The ICT Sector Working Group[6] involves only government and international donors. The US Embassy has initiated the US ICT Council for Myanmar with support from the Myanmar Computer Federation. Under the Open Government Partnership, the government must consult civil society on its action plan. However OGP does not cover all the issues relevant to building appropriate safeguards into the ICT sector. At this stage, there are still opportunities to shape the long-term direction of the sector, learning lessons from elsewhere. Developing a multi-stakeholder discussion on the ICT sector could help further focus the Government's commitment to implement a people-centred approach, in line with growing international developments on a balanced approach to Internet governance.[7] The Myanmar Centre for Responsible Business (MCRB) stands ready to support such dialogues.

4. Initiate and support efforts to educate the Myanmar public about safe and peaceful behaviour online, including counter-speech.

There is a clear role for civil society in helping to educate users on the dangers and opportunities of accessing ICTs in Myanmar. Given the wide range of languages in the country, it would be particularly useful for civil society organisations to make available information in Burmese and other languages, including clear and accessible explanations, training, awareness raising campaigns, etc. There is also a clear role for civil society in responding to and countering "hate speech", and providing concrete examples where online communities can support efforts around peaceful expression.

5. Increase media reporting on ICT sector.

Given the importance of the ICT sector to Myanmar, media outlets should increase informed reporting on the sector and its impacts to improve transparency, company and Government accountability, and public understanding. This should include reporting on complex and hidden areas such as the Government's lawful interception policies and practices.

[6] See "Sector working groups dashboard".
[7] See for example the Global Commission on Internet Governance.

Recommendations

To Development Partners & Home Governments

1. Support the strengthening of human rights, social and environmental considerations within ICT policy, legal and regulatory improvements, especially those highlighted in Recommendations 2 and 3 to the Myanmar Government.

Key Points for Implementation

- **Support the Myanmar Government to introduce of an effective framework for the ICT sector that includes adequate safeguards.** A number of partners including the Asian Development Bank (ADB), the World Bank, and the European Union (EU) are working on parts of the ICT regulatory framework. Given the past history of the country, it will be important to support the Government through both appropriate technical advice and political messaging, to ensure that the regulatory frameworks being put in place appropriately safeguard human rights. Any revised frameworks being supported with donor funding should not facilitate a return to excessive surveillance and repression. This might occur, for example, if the regulatory framework has been too broadly worded and allows wide latitude in interpreting and implementing the law. Development partners should ensure that the consultants hired by them or through the international financial institutions can and do provide appropriate advice, not only on technical matters but also on the balance to be struck in regulatory frameworks to ensure human rights are safeguarded.
- **Monitor whether the Government has developed its regulations on lawful interception** in line with international standards and good practice as set out in the Annex to the Recommendations.
- **Support rule of law changes to develop on-going checks and balances in the system** necessary to ensure implementation of an adequate ICT regulatory framework with appropriate safeguards. For example, the Government has indicated that it will require judicial review of lawful interception requests made by the Government. That is an important step, but it will be important to ensure that judges receive appropriate training and are part of a broader programme to strengthen the rule of law in Myanmar.
- **Support programmes to develop civil society capacity** to engage effectively with the Government on the extensive ICT reforms and with ICT companies (see Recommendations to CSOs, Human Rights Defenders & the Media above).
- **Support programmes to develop media capacity to report on ICT issues.**
- **Encourage the international financial institutions (IFIs)** working on ICT sector reform in Myanmar to make information and expertise available in order to engage a wider portion of Myanmar civil society and the population on the work they are doing.

2. Support implementation of the corporate responsibility to respect human rights by Myanmar and international companies.

UN Guiding Principles on Business and Human Rights: The State Duty to Protect

2. States should set out clearly the expectation that all business enterprises domiciled in their territory and/or jurisdiction respect human rights throughout their operations.

Key Points for Implementation

- **Home country governments should proactively express their expectations of companies domiciled in their country that are investing, or are looking to invest, in Myanmar.** This should include clear expectations that they should operate in line with the UN Guiding Principles on Business and Human Rights and, where relevant, the OECD Guidelines on Multinational Enterprises, including the requirements on disclosure. They should encourage companies to apply the IFC Performance Standards and WBG Environmental, Health and Safety Guidelines in the absence of Myanmar laws that provide for a higher standard.
- **Consider adopting reporting requirements modelled on the US Reporting Requirements on Responsible Investment in Burma**, or other reporting requirements for companies on environmental, social and human rights impacts (such as in the EU), and encourage companies to report specifically on Myanmar as a high-risk country for human rights.
- **Support the Government of Myanmar** in **introducing standards for responsible business conduct** for companies operating in Myanmar (See Recommendations to the Myanmar Government above).

3. Ensure investment and free trade agreements negotiated with the Government of Myanmar reinforce responsible business practices.

UN Guiding Principles on Business and Human Rights: Ensuring Policy Coherence

9. States should maintain adequate domestic policy space to meet their human rights obligations when pursuing business-related policy objectives with other States or business enterprises, for instance through investment treaties or contracts.

Key Points for Implementation

- **Ensure that investment, free trade, and other international economic agreements are coherent** with each country's or inter-governmental organisations' (in the case of the European Union) international obligations, including its international human rights treaty obligations, and make reference to the UN Guiding Principles on Business and Human Rights.
- **Ensure that each party to such agreements has preserved sufficient "policy space"** (freedom to make policy changes and choices after the agreement is formalised) for further changes to domestic policy that can improve environment, social and human rights protections. Governments should ensure that those agreements reinforce rather than restrict good governance and responsible business practices.

Recommendations
To Investors

1. Conduct due diligence on companies in portfolios that are involved in the ICT sector in Myanmar.

This should include enhanced due diligence regarding their policies, systems, reporting and responses to specific human rights challenges in Myanmar. Investors should understand if the companies they invest in are creating risks to human rights and if so, the steps the companies are taking to prevent and mitigate those risks and remedy impacts.

2. Engage with investee companies involved in the ICT sector in Myanmar to ensure that these companies meet international standards on responsible business conduct relevant to their business in Myanmar.

This might involve direct engagement or participation in shareholder actions.

3. Urge companies doing business in the ICT sector in Myanmar to report robustly on how they manage risks and impacts associated with investments and operations in the country.

The US Government's Reporting Requirements on Responsible Investment in Burma could be used as a framework for such disclosures.

Recs

Recommendations
To Users

1. Undertake basic steps to protect your privacy and security while using ICTs.

- **When using social media:**
  - **Avoid publicly** sharing personal information such as bank statements, address, email address, date of birth or mobile phone numbers on social media or mobile applications.
  - Use privacy **settings** to control what other users can see or access on your profile.
- **When using online services:**
  - Use **strong passwords**, which: [8]
    - Are at least eight characters long
    - Do not contain your user name, real name, organisation name, or a complete word
    - Are significantly different from previous passwords
    - Contain uppercase letters, lowercase letters, symbols and numbers
  - **Avoid using the same password for different services, e.g. Facebook and Gmail**.
  - Keep these passwords **safe and confidential**.
- **When using email:**
  - **Avoid** opening emails with **file attachments from unknown senders**.
  - Use a **different email address** for online services than the email address used for personal email communication.
- **When browsing the Internet:**
  - Use **"private browsing" settings** in Chrome, Firefox, Safari, or Internet Explorer. Private browsing prevents websites from remembering your login information and prevents your browser from logging websites you visit under your browsing history.

[8] Microsoft, "Tips for Creating a Strong Password" also see Micah Lee, The Intercept, Passwords you can Memorize- But That Even The NSA Can't Guess (26 March 2015) for additional guidance on designing strong passwords.

Annex to the Recommendations

Lawful Interception and Government Access to User Data: The Characteristics of a Rights-Respecting Model

Purpose

At the time of this report, a key part of Myanmar's telecommunications framework on lawful interception (LI) had yet to be finalised. Regulators need to define the limits of lawful communications surveillance and clarify the capabilities and the uses of communications surveillance technology used for lawful interception, which refers to access of communications content in real time. The section below lays out the characteristics of a framework that protects human rights to cover both lawful interception and government access to user data. Both are considered to be acts of surveillance.

The distinction between lawful interception and access to user data is that lawful interception covers real time access to communications and access to user data is about historical data, known as "communications data".[9] In many countries the laws governing what can be accessed, and when, make distinctions between the two, with a higher burden of proof to authorise lawful interception.

In recent decades, both physical and communications surveillance was widely conducted in the absence of a legal framework or oversight. There is an opportunity for the Government of Myanmar to develop legal protections that respect human rights, as part of the wider 'people-centred' reforms, and to take a leadership position within the region. Such a lawful interception framework will build trust in the use of Myanmar's ICTs among users, service providers and other governments by being robust and aligned with international human rights standards.[10]

As outlined above, the only existing legal framework is Article 75 of the 2013 Telecommunications Law, which allows interception but does not clearly articulate definitions or justifications.[11] The Government of Myanmar has asked the European Union for technical assistance in drafting implementing legislation. To assist this drafting

[9] Communications Data (sometimes referred to as metadata) is basically everything but the content and includes telephone numbers of both the caller and the recipient, the time and duration of a call, unique identifying numbers (each subscriber is allocated one, as is each mobile device), email addresses, web domains visited and location data. This information is important as it builds up a detailed picture of a person's life and movements, so that often intercepting the content of a call or email is not necessary. In contrast to content, there are often weaker legal protections around interception of stored communications data.

[10] See for example: See for example the Global Conference on Cyberspace 2015, the Global Commission on Internet Governance

[11] Article 75 states: "*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."* See unofficial English translation of the Telecommunications Law (2013)

process, MCRB has conducted preliminary research into what the characteristics of a human rights respecting model of lawful interception might look like in Myanmar. These findings are presented below and aim to provide useful information to the Government of Myanmar and other stakeholders involved in drafting this legislation, including the 2016 Parliament.

These recommendations[12] set out the principle considerations as the Government of Myanmar begins to develop an approach to regulation and legislation on communications surveillance covering 7 main issues:[13]

The Characteristics of a Rights-Respecting Lawful Interception Model

1. Prerequisites
2. Authorisation Processes
3. Oversight
4. The notification of individuals
5. Remedy
6. Transparency
7. Provision for Framework Review

1. Prerequisites Before Lawful Interception Should be Considered

- Lawful interception should be undertaken only when other potential measures that could have been used to deal with the criminal or national security threats have been exhausted, for example other police measures that do not involve surveillance.
- Any type of surveillance should be carried out only on targeted suspected individuals and organisations where there is prior suspicion that the targeted subject is suspected of a crime.[14]
- Misuse of intrusive capabilities should be a criminal offence and surveillance used outside the legal frameworks should be prohibited.
- The legal framework authorising lawful interception and access to user data should be established through primary legislation and debated in the legislative branch, rather than being adopted as subsidiary regulations enacted by the executive. Public consultation and involvement of stakeholders is a vital part of the policy-making process because many of the processes under the legislation will be carried out behind closed doors, without the opportunity for public scrutiny. It is even more important therefore that the public has a say in establishing the framework.
  - The Government of Myanmar has committed to a public consultation of draft lawful interception regulations.[15]

[12] These recommendations draw on recent reports to the UN General Assembly and Human Rights Council, including the Report of the UN Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression A/HRC/23/40 (June 2013); The Right To Privacy in the Digital Age, UN Resolution 68/167 adopted 21st January 2014 ; Report of the Office of the United Nations High Commissioner for Human Rights, presented to the Human Rights Council in September 2014 A/HRC/27/37 and the Report of the UN Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism to the UN General Assembly in September 2014 A/69/397

[13] The issues addressed cover both lawful interception (real time access to communications) and access to historical data (which has a number of different terms in law in different jurisdictions including communications data and metadata,

[14] See: UN General Assembly A/69/397 23rd September 2014

[15] See the announcement on p5 of the Public Consultation Issued by the Ministry of Communications and Information Technology of the Republic of the Union of Myanmar. Proposed Rules for Telecommunications

2. Authorisation Processes

- Specific instances of communications surveillance should be authorised by an **independent** and **competent** judicial authority prior to surveillance taking place. Some states have a process of executive sign-off rather than judicial authorisation.
- **Independence** in this circumstance means separate and not connected to the authorities that will be carrying out the surveillance. **Competence** means that those with responsibility for giving authorisation must have sufficient knowledge of the issues, both technologically and from a human rights perspective. This independence and competence is absolutely critical to the integrity of any legal framework. Some states have a process of executive sign-off rather than judicial authorisation. But the prevailing view at the UN level and among civil society is that judicial authorisation is preferable for its independence (the Authorising Authority).
  - The Government of Myanmar has already committed to judicial authorisation.[16]
- Communications surveillance must be limited to that necessary to achieve a legitimate aim and use the means least likely to infringe rights; it must be both necessary and proportionate. An objective assessment of the necessity and proportionality of the contemplated surveillance should be a core part of the authorisation process.
- The legal framework should set out which agencies among government bodies can request lawful interception (the Requesting Agencies).
- The legal framework should also set out the criteria and conditions on which the court will make the decision on whether to authorise the request.
- Any authorisation should be time-bound with a requirement for the Requesting Agency to return to the Authorising Authority to request a renewal as that period of time expires; automatic renewals of surveillance requests should not be permitted.
- The legal framework should set out clear limits on the amount of time that data collected can be stored. It should require that data is destroyed once the period expires. In addition, it should require that any data illegally collected is immediately destroyed and not used.

3. Oversight

- There is an on-going global debate about the best form of oversight of lawful interception and access to user data. Increasingly there is interest in mixed models of oversight that incorporate administrative, judicial and parliamentary actors.
- Oversight must be vested in another body (or bodies) that is independent of the Authorising Authority that originally authorised the surveillance.
- Oversight must be rigorous and not a rubber stamping exercise.
- Consideration should be given to permitting a confidential public interest advocate, for example an independent human rights expert, within the surveillance authorisation process to ensure that appropriate consideration is given to the human rights implications of the request. This is particularly important given the high degree of secrecy of authorisation processes that relate to national security.
- The oversight body must have access to all potentially relevant information to enable it to evaluate whether the government is carrying out its activities in a lawful way. This must include secret and classified information. Third parties, for example companies, should have the ability to bring relevant information to the oversight body.
- The oversight body must have the resources and expertise to be able to carry out effective oversight.

Sector Relating to Licensing, Access and Interconnection, Spectrum, Numbering, and Competition (November 4, 2013)

[16] Telenor Myanmar sustainability presentation (August 19th 2014). See p8 of the transcript.

- Within the oversight regime there must be regular reporting to the public on whether the government is carrying out its surveillance activities appropriately, in a way that helps the public understand whether the government has followed the procedures.
- Oversight will usually happen at a defined time after surveillance has taken place (often with a regular report to the Parliament or public) and is designed to test whether surveillance that has already happened took place in accordance with the framework the country has in place.

4. Notification of Individuals under Surveillance

- It is understood that there will be times when individuals cannot be notified that they are under surveillance as to do this could jeopardise the surveillance itself.
- However, notification of individuals if they have been the subject of surveillance is an important part of the framework in a country to give individuals who may have been subject to illegal surveillance access to remedy**.** At a minimum, users should be notified that their communications have been subject to surveillance when the surveillance is complete.
- The legal framework should set out the circumstances under which there may be a delay in individuals being notified that they are under surveillance and the authorising body for this.

5. Remedy

- Individuals need to know whether they have been the subject of surveillance in order to bring a complaint and obtain a remedy for surveillance that was carried out not in accordance with the law. When individuals are informed that they have been the subject of surveillance they should also be informed of the procedure for filing a complaint if they wish to do so,
- Any alleged violation must be promptly, thoroughly and impartially investigated.
- Where a violation is identified it must be possible to end it. For example, the body examining the potential abuse must be able to order the termination of the surveillance and the deletion of data and prohibition of its use by issuing binding orders.

6. Transparency

- The legal framework concerning communications surveillance must be publicly accessible and set out the nature, scope and time-frame of possible surveillance, the requirements that must be met for surveillance to be authorised, and which authorities are responsible for authorisation, carrying out and supervising the surveillance. The process for remedy for individuals who have been the subject of inappropriate surveillance must be explained, as should the circumstances in which there can be sharing of information across borders between governments. There should be a clear explanation of each different type of surveillance that is possible. See below for some of the current issues that are being addressed in international and national debates relating to this.
- The publicly accessible information about surveillance set out in the law must be sufficiently clear and precise for individuals to be able to understand it and foresee how the law might be applied to them.
- To promote government accountability, the government should produce, as a minimum, the aggregate yearly figures on the specific number of requests for surveillance it has made, including the number accepted and rejected, details of the way in which it has been using its powers, and information broken down by specific legal authority for example, wiretaps, the number of requests to service providers, etc.

7. Provision for Periodic Review of the Lawful Interception Framework

- Given the speed at which technology develops, and the potential for communications surveillance to infringe rights, it is important that there is provision within the legislative or regulatory framework for periodic review of the law to ensure rights are protected.

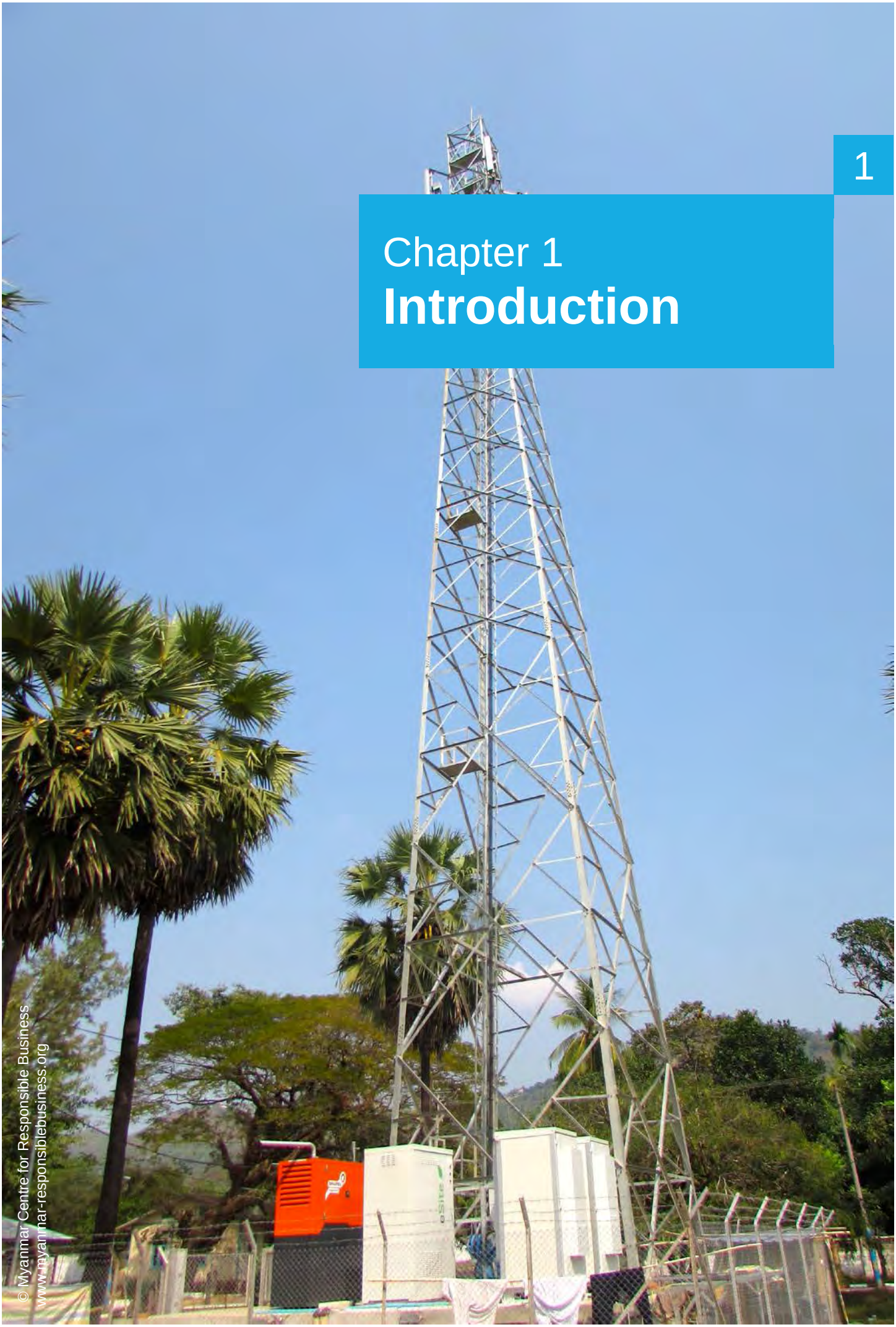
Other Considerations to Take into Account in Drafting the Legal Framework

- **Consistency between the regulation, law and practice:**
  - Embedding human rights principles into the regulation and laws that provide the framework for interception and surveillance is insufficient on its own.
  - The agencies requesting surveillance must be required to consider the human rights implications in the requests that they make. This should include consideration of whether any less intrusive methods are possible, to ensure that the issue of proportionality is addressed.
  - There should be training on the human rights implications and their obligations to consider them for all agencies who have the powers to make requests. Training the judiciary is also required.
  - Accompanying the legal framework there should be a more detailed code of practice that sets out how the law is intended to work in practice.
  - Where there is more than one law or regulation in place (e.g. telecoms law, national security law, tax, drug enforcement, cybersecurity legislation etc.) there must be consistency in the human rights safeguards in place and clarity provided on which law has primacy in which circumstances.

- **The role of companies providing service to users:**
  - Service providers should not be compelled to modify their infrastructure to enable direct surveillance that eliminates the opportunity for judicial oversight.
  - Any request to service providers for access to communications content or data should be provided in writing, explaining the legal basis for the request including the requesting government entity and the name, title and signature of the authorised official. Although it is preferred for requests to be provided in writing it is recognised that there are certain exceptions provided for by law, for example emergency situations and immediate risk to life where oral requests are acceptable, providing they are followed up in writing.
  - Service providers should have the right to seek clarification or modification to a request which does not seem to follow domestic legal procedures (which in turn should incorporate the internationally accepted human rights protections).

- **Areas of Current International and National Debate on Lawful Interception:**
  - Many countries require a higher degree of authorisation for access to communications content than they do to access communications data or metadata. Metadata / communications data can give more insight into a person's life than was historically the case with simple telephone call and duration information, for example, mobile location data. This has resulted in an active debate about whether this lower level of protection that is given to communications data or metadata is still appropriate. Some countries have recommended the consideration of a third category of data, in addition to communications content and metadata/communications data. This proposed third category would give greater protection to certain types of communications data considered more sensitive, such as websites visited and a user's location from a smartphone.
  - The leaks from Edward Snowden regarding the surveillance activities of the US National Security Agency (NSA) and the UK Government Communications Headquarters (GCHQ) have put the spotlight on "mass surveillance." There is no international agreement on what this term means in different jurisdictions. At the UN level there is serious concern about communications surveillance authorised on such a broad and indiscriminate basis. This runs counter to the core concept of the protection of privacy that requires justification to be made on a case-by-case basis.
  - The issue of whether nationals of a particular country should enjoy higher protection than non-nationals is a current debate. The International Covenant on Civil and Political Rights (ICCPR) by its terms provides protection to all, without distinction based on nationality.
  - Laws that authorise extra-territorial surveillance or the interception of communications in foreign jurisdictions are problematic, for example because of an individual's inability to know if they are subject to surveillance and therefore potentially seek redress.

Chapter 1
Introduction



1

Chapter 1
INTRODUCTION

In this Chapter:

A. Why an ICT Sector-Wide Impact Assessment (SWIA) in Myanmar

Myanmar currently has one of the least developed ICT sectors in ASEAN. However, concerted efforts are underway to rollout an extensive telecommunications network to spur the development of the ICT sector and enable other industries dependent on modern communications to flourish. It is estimated that by 2030 the ICT sector could contribute $6.4 billion to Myanmar's GDP and employ approximately 240,000 people.[17] With foreign investment in the telecommunications sector estimated to contribute over $2 billion of $8.1 billion in total FDI in 2014/2015,[18] Myanmar is finally bridging the 'digital divide'.

ICT is considered a high-risk sector for human rights. Certain impacts of the ICT industry on human rights have been well documented, for example, working conditions in hardware manufacturing.[19] However, other types of impacts, particularly on freedom of expression and privacy, have only come into focus more recently.

Emerging from decades of ethnic conflict, authoritarian rule and a long period of economic sanctions, Myanmar is considered a high risk destination. As investments in the sector are increasing rapidly, all stakeholders – companies, Government, civil society and donors – need to understand the potential impacts of the sector if it is to improve the outcomes for Myanmar and all of its people. This Sector Wide Impact Assessment (SWIA) aims to aid that understanding.[20]

The ICT sector is often described as a complex 'ecosystem'. Its elements range from telecommunications service providers to large equipment manufacturers to small software

[17] See, McKinsey Global Institute, "Myanmar's Moment: Unique Opportunities, Major Challenges" (June 2013), pg 3.
[18] Deal Street Asia, "Myanmar 2014-2015 FDI swells to $8.1b: govt agency" (April 2015).
[19] Report of the Special Representative of the Secretary-General on the issue of human rights and transnational corporations and other business enterprises (herein "SRSG"), "Addendum, Corporations and human rights: a survey of the scope and patterns of alleged corporate-related human rights abuse", A/HRC/8/5/Add.2 23 (2008).
[20] MCRB, IHRB and DIHR have already carried out two other SWIA on important areas of the Myanmar economy – oil and gas and tourism.

or web-based startups. Individual companies in the sector may also play multiple roles, for example, manufacturing mobile phones and network components, or providing both mobile telecommunications and Internet access services.[21] Chapter 3 provides a brief description of the ICT value chain and the kinds of companies (foreign and national) involved in Myanmar's ICT sector. This SWIA for the ICT sector looks at the entire value chain of ICT activities in Myanmar, other than manufacturing which is very limited in Myanmar. It includes some focus on the telecommunications operators, infrastructure and network equipment providers, and some 'over the top' web-based service providers in Myanmar – both local Myanmar companies as well as foreign companies.

The SWIA does not address technical operating standards for the ICT industry. Instead, it looks at the sector through the lens of responsible business and the international standards that set out the expectations for responsible business (See Section B below). It involves assessing impacts on individuals and groups that may arise from individual projects and operations in the sector as well as the sector's potential impact on the society as a whole. It is set in the context of the current operating environment in Myanmar. A SWIA is intended to sensitise planners, decision-makers, businesses and civil society, including the media, by highlighting the likely risks and impacts of business activities in the ICT sector, so that appropriate steps can be taken at an early stage to prevent and mitigate risks and amplify positive human rights impacts through changes in policy, law, contracts, operations or other relevant measures.

Uses for the ICT SWIA

Because a SWIA is a new concept and because human rights issues round the ICT sector are relatively unknown in Myanmar, the SWIA report (the Report) is extensive and provides detailed explanations of the core human rights considerations to contribute to the knowledge base in the country. Targeted at multiple audiences, it aims to:

- **Inform companies** conducting operational-level due diligence and help them understand the overall potential impact of their sector and their operation(s) on the country and on human rights in particular. The SWIA provides a strategic review of the broader policy and legal frameworks relevant to the sector, their implications for businesses, and their impacts on human rights and society. It also crystallises the acute issues that are central to operating in Myanmar and require proactive management by ICT companies. It highlights a number of issues that will be best served if tackled collectively. Readers from business, who are keen to understand the immediate implications for them are encouraged to read in particular the 'Recommendations for ICT companies' in the ten sections of Chapter 4 on Operational Level Impacts.
- **Help the Government and Parliamentarians** as they shape ICT-relevant policy and law, enforcement and other initiatives to better prevent and mitigate human rights harms and enhance the potential for positive outcomes. Adequate attention to longer-term

[21] For a broader understanding of the ways in which the ICT sector can impact human rights, and how the UN Guiding Principles can be operationalised, see: European Commission, "ICT Sector Guide on the UN Guiding Principles on Business and Human Rights" (2013).

impacts on human rights supports more equitable growth and poverty reduction for the broader Myanmar population.

- **Support local communities and users** to engage with companies and the Government and to enable them to call on international standards to support their engagement.
- **Support trade unions, workers, civil society organisations** so that they can participate in policy development and project planning, leveraging international standards and approaches in their interventions.
- **Inform the media** so that they can report effectively on policy and legislative developments and promote user understanding of ICT.
- **Enable development partners** to align their support and policies to the sector such that human rights are better respected and protected.
- **Build the capacity of local researchers** to better understand international standards relevant to operations of the sector in Myanmar and to be able to assess performance in light of those standards.

See Annex A for a more detailed description of the SWIA methodology and scope and coverage of the field research carried out. The data from the field research is purposefully anonymised to focus attention on trends in the ICT sector as it continues to develop. **The research findings should not be taken to apply to all situations, organisations, or companies interviewed.**

B. Expectations of Responsible Business Conduct in Myanmar

This SWIA sets out some of the many challenges and opportunities of operating in Myanmar. It presents the context that companies must either change, where appropriate, or adapt to, in order to run operations in a responsible manner, rather than simply accepting the deficiencies as they are. Companies operating in a high-risk environment have a particular responsibility to influence that operating environment, within the bounds of their own impacts (which may be broader than just their own operations) by operating according to international standards. Where appropriate, this includes engaging with the Myanmar national and local governments, quietly, collectively or even publicly, to prompt them to take up those same standards. It also includes engaging on broader issues that can affect the business environment and society: peace, security, human rights, good governance. A transparent approach to applying international standards on responsible business conduct will help provide a common baseline for all. The choices companies make in responding to these conditions will play a major role in whether the ICT sector is seen as a positive contributor to national development in Myanmar.

Expectations of the Myanmar Government

President U Thein Sein, Daw Aung San Suu Kyi (leader of the opposition National League for Democracy (NLD)), numerous governments and international organisations, have all called for 'responsible business' in Myanmar. Together with the OECD, the Government conducted an 'investment policy review' of the country in 2013. The 300+ page report starts with a chapter on responsible business, focused on human and labour rights and how international standards of responsible business conduct can be introduced in the country (See Table 1 below).[22] In discussing the report, the Myanmar's Union Minister of National Planning and Economic Development, Dr Kan Zaw, "*praised the comprehensive nature of the report and said that it would help to guide the Government in solidifying investment climate reforms and in promoting more and better investment*."[23] This points to a Government interested and willing to align itself with international standards.

Table 1: Recommendations from the OECD as part of the Myanmar Investment Policy Review Chapter on Responsible Business Conduct[24]

- Ratify major international human rights, labour and environmental conventions
- Enact and enforce domestic legislation consistent with these standards
- Strengthen the independence and expand the mandate of the National Human Rights Commission
- Promote revenue transparency
- Ensure that domestic enterprises, including state owned enterprises, conform to the new standards of behaviour and prosecute lawbreakers
- Expand the role of civil society (labour unions, local community organisations) to help ensure that businesses obey the law
- Prepare sectoral master plans which include responsible business conduct (e.g. tourism)
- Provide adequate protection of property rights, including for customary land
- Free, prior and informed consent (FPIC) for land acquisitions, relocations, etc.
- Develop grievance mechanisms in other areas and provide redress to victims
- Work with home governments to promote respect for the UN Guiding Principles on Business and Human Rights and the OECD Guidelines for Multinational Enterprises. Require foreign investors receiving a permit from the MIC to commit to these principles.

However, the hard work of translating those commitments into relevant laws, policies and practices throughout the country is just beginning. The legacy of over fifty years of military Government and isolation will have to be addressed to ensure that the benefits of a modern telecommunications network and ICT sector contribute to widespread development. While Myanmar has taken significant steps towards reintegration into the global community, it is still a 'high risk' or 'weak governance' country, requiring a higher level of rigour and sensitivity in conducting business. Entrenched elite interests, widespread corruption, lack of state capacity and a lack of comprehensive social policies have led to low levels of state legitimacy, social cohesion and trust. While high-risk

[22] OECD, "OECD Investment Policy Reviews: Myanmar 2014" (March 2014).
[23] ASEAN Secretariat, "Myanmar Welcomes International Support for Responsible Investment" (March 2014).
[24] OECD, "OECD Investment Policy Reviews: Myanmar 2014" (March 2014) pg. 32.

countries like Myanmar badly need investment, companies can cause detrimental economic, social and political impacts if their operations are not carried out responsibly.

Expectations of Home Governments

Home governments also play a key role in encouraging and incentivising the behaviour of companies based in their jurisdiction and operating abroad. In lifting its sanctions on Myanmar, the EU noted that it would "*[p]romote the practice of the highest standards of integrity and corporate social responsibility*". [25] In 2013 the G8 welcomed the Government's commitment to responsible investment.[26] The US's Burma Responsible Investment Reporting Requirements (see Table 2 below) are, however, the only example to date of explicit home country requirements on businesses investing in Myanmar[27]. They are intended to prompt businesses entering the country to consider and address key risks upfront.

Table 2: US Reporting Requirements on Responsible Investment in Burma

Companies subject to the US reporting requirements must, inter alia notify the US Department of State of their policies and procedures on human rights, labour rights, land rights, community consultations and stakeholder engagement, environmental stewardship, anti-corruption, arrangements with security service providers, risk and impact assessment and mitigation, payments to the Government, and any investments with, and contact with, the military or non-state armed groups.[28]

International operators are expected to act as industry leaders on environmental, social and human rights performance in Myanmar. There is intense scrutiny of companies entering or operating in Myanmar, with a particular focus on whether they are operating in line with the UN Guiding Principles on Business and Human Rights[29] and other relevant international standards. To fully understand the direct and indirect risks that arise from weak governance, enhanced due diligence is needed to understand and manage those risks.[30] As noted in OECD guidance on weak governance zones, "*because legal systems and political dialogue in weak governance zones (almost by definition) do not work well, international instruments that provide guidance on acceptable behaviours are particularly useful in these contexts*."[31] Due to most companies from OECD countries staying out of Myanmar prior to 2012, few companies have yet faced 'specific instances' claims under

[25] Council of the European Union, "Council Conclusions of 22 July 2013 on the Comprehensive Framework for the European Union's policy and support to Myanmar/Burma" (2013). The Council Conclusions go on to name the OECD Guidelines for Multinational Enterprises, UN Guiding Principles on Business and Human Rights and the EU CSR Strategy 2011-2014 as sources of these standards.
[26] UK Foreign & Commonwealth Office, "G8 Foreign Ministers' meeting statement" (April 2013).
[27] US Department of the Treasury, Office of Foreign Assets Control (OFAC) "Burma Responsible Investment Reporting Requirements" (2012).
[28] TPG Holdings I, filed a report on behalf of TPG Growth II, which jointly owns Apollo Towers Myanmar Ltd.with TPG Asia VI, L.P. It is the only company in the ICT sector to have filed a report so far under the US Reporting Requirement.
[29] Office of the High Commissioner for Human Rights (OHCHR), UN Guiding Principles on Business and Human Rights (2011)
[30] IHRB, "From Red Flags to Green Flags, The Corporate Responsibility to Respect Human Rights in High-Risk Countries" (2011), pg. 21.
[31] OECD, "OECD Risk Awareness Tool for Multinational Enterprises in Weak Governance Zones" (2006).

the OECD Guidelines on Multinational Enterprises procedures for their actions in Myanmar. None has yet involved the ICT sector, though several 'specific instances' concerning ICT in other countries have been lodged[32].

Expectations of Investors

Investors are demanding information on company actions in Myanmar. Investment research providers are now providing specialised information on Myanmar.[33] As one investor blog notes, *"[c]ompanies investing in Burma are exposed to a complex business environment and those that are seen to benefit from violations of human rights face serious reputational risks".*[34]

C. The Reference Framework for the SWIA

The language and meaning of 'human rights' and 'responsible business'

'Responsible business conduct' and the standards that help define that conduct, require businesses to take responsibility for the impacts they have on society. 'Impacts on society' is understood very broadly to include human rights, and social, environmental, ethical, and consumer concerns. The standards that cover such conduct are diverse and they are not always labelled as 'human rights', but they are intimately intertwined with human rights.

Some impacts on human rights will be **direct**. Suppression of a protest by a company has an immediate impact on the right to freedom of expression. Other impacts may be **indirect**. Pollution can degrade the quality of the soil or water so that crops can no longer be grown or grown in sufficient quantities, impacting on the right to food. Wider governance issues, including corruption and a lack of transparency[35] have indirect impacts as they can weaken the systems needed to hold those responsible for abuses accountable, and to provide remedies to victims.

When the 'human rights' label or terminology becomes a stumbling block to positive outcomes, the use of other terms may be appropriate. But it will still be important for those dealing with these issues in companies and with stakeholders, to have an understanding of internationally-recognised human rights and their implications for company processes in order to ensure that a company is indeed meeting responsible business standards.

---

[32] Lists of 'specific instances' by country and sector can be generated at http://oecdwatch.org/cases

[33] EIRIS, "New service enables investors to manage conflict-related investment risks in Burma/Myanmar" (May 2014).

[34] EIRIS, "An Australian perspective on human rights, conflict risk and investment" (June 2014).

[35] While this SWIA addresses corruption because it has an impact on the quality of governance more generally and the resources governments have available to fulfil human rights, it does not include a specific review of all the steps that would be needed to reduce corruption in the country. See for example, Devex, "How Myanmar can curb corruption to boost development" (30 Jan 2014).

1

The Key International Standards as a Framework for the SWIA

As the ICT SWIA is particularly focused on human rights, the UN Guiding Principles on Business and Human Rights (the UN Guiding Principles)[36] are its primary benchmark. These were unanimously endorsed by the UN Human Rights Council in 2011 and are now the authoritative global reference point on business and human rights. The UN Guiding Principles provide operational guidance to States and business for the implementation of the UN 'Protect, Respect and Remedy' Framework (2008) [37] which defines the complementary but distinct roles of States and business in protecting and respecting human rights. At a minimum, business must ensure that its activities do not infringe the human rights set out in the International Bill of Human Rights,[38] the principles concerning fundamental rights set out in the International Labour Organisation's Declaration on Fundamental Principles and Rights at Work,[39] as well as other human rights instruments concerning specific vulnerable or marginalised groups which a company may adversely impact.[40]

The ICT SWIA also incorporates other key international standards relevant to responsible business conduct, particularly those concerning impacts of business on human rights:

- The **OECD Guidelines on Multinational Enterprises** which apply to the global operations of companies domiciled in an OECD country and the 10 additional countries adhering to the OECD Guidelines.[41] The human rights chapter of the OECD Guidelines on Multinational Enterprises is aligned with the UN Guiding Principles. The OECD Guidelines therefore apply to the Myanmar operations of any company based in any of the 45 countries adhering to the Guidelines.
- **ISO 26000 and the UN Global Compact** are also aligned with the UN Guiding Principles and important references in the region.
- sustainability policies of international financial institutions (Asian Development Bank and World Bank Group), and in particular, the **IFC Performance Standards** and **World Bank Group Environmental, Health and Safety (EHS) Guidelines**. The IFC Performance Standards and EHS Guidelines are designed to be applied by the private sector, contain quite detailed standards for many areas relevant to ICT operations, and specifically cover and are aligned with many human rights standards.
- guidance from leading industry groups such as Global Network Initiative (GNI), Telecommunications Industry Dialogue, and Global e-Sustainability Initiative (GeSI).

[36] See: OHCHR, UN Guiding Principles on Business and Human Rights (2011).
[37] See: OHCHR, UN "Protect, Respect and Remedy" Framework (2008).
[38] Comprised of the UN Declaration on Human Rights, the International Covenant on Civil and Political Rights, and the International Covenant on Economic, Social and Cultural Rights.
[39] International Labour Organisation's Declaration on Fundamental Principles and Rights at Work (1998).
[40] See: OHCHR, "The Core International Human Rights Instruments and Their Monitoring Bodies" (accessed August 2015).
[41] Additional signatories to the OECD Guidelines are: Argentina, Brazil, Colombia, Egypt, Latvia, Lithuania, Morocco, Mexico, Peru, and Tunisia. See: http://mneguidelines.oecd.org/ncps/

Building on the UN Guiding Principles on Business and Human Rights

The process of field research and consultation leading up to the SWIA publication and its subsequent dissemination are designed to support the implementation of the UN Guiding Principles within Myanmar as follows:

- **Pillar I: The State Duty to Protect** against human rights abuses by third parties, including businesses, means the State should adopt effective policies, legislation, regulations and adjudication to prevent, investigate, punish and redress human rights abuses as a result of domestic business operations. As the Government of Myanmar and Parliamentarians develop sectoral policies and laws, they will be making choices about the future direction of the country, balancing potential negative and positive impacts of their decisions. The ICT SWIA provides an analysis that helps inform law, policy and administrative procedures in ways that prevent and mitigate harms and enhance positive outcomes. Foreign governments supporting economic development in Myanmar can also use the SWIA to better understand the human rights impacts of the ICT sector in Myanmar, and align their foreign investment support and policies.
- **Pillar II: The Corporate Responsibility to Respect** human rights, means that companies should avoid infringing the human rights of others and address negative impacts with which they are involved. The ICT SWIA provides a better understanding of potential human rights impacts at the operational level and a preview of factors contributing to a sectoral 'social license to operate'. This should assist ICT companies into incorporating attention to human rights issues into their own human rights due diligence around their investments and operations (See Table 3 below).
- **Pillar III: Access to Effective Remedy** for victims of business-related human rights abuses should be provided through both judicial and non-judicial means. While the ICT SWIA is not a comprehensive review of rule of law and access to justice in Myanmar, it provides a brief overview of the currently limited avenues for access to effective remedy in Myanmar. It therefore encourages businesses to put in place grievance mechanisms that enable users, communities and workers to raise their concerns regarding ICT sector impacts, in order that they can be addressed as early and effectively as possible. As such, the SWIA supports workers, users and local communities in understanding and protecting their rights.

The Corporate Responsibility to Respect Human Rights

Companies should not assume that complying with Myanmar national law will be sufficient to meet the responsibility to respect human rights. The evolving domestic legal framework still lags behind international standards, and compliance with national law is unlikely to be sufficient to meet international standards in many areas.

The UN Guiding Principles and the OECD Guidelines on Multinational Enterprises require companies to assess and manage their potential adverse impacts as a core part of meeting the corporate responsibility to respect human rights. Being as transparent as possible, including communicating the dilemmas they face and the measures they are

taking to address them is part of 'knowing and showing' that a company is taking steps to respect human rights.[42]

Table 3: The Corporate Responsibility to Respect Human Rights

Under the UN Guiding Principles on Business and Human Rights, companies are expected to respect human rights. That means companies should avoid infringing on the human rights of others and address negative impacts with which they are involved. In order to be able to 'know and show' that they are indeed avoiding negative impacts on human rights, companies should take the following steps:

- Adopt a **policy commitment** that commits the company to respecting human rights (this may be a standalone commitment or integrated with other commitments to responsible business conduct)
- Carry out **human rights due diligence** (which can be integrated into other types of due diligence procedures that assess and manage the company's impacts on society and the environment).[43] This includes:
  - **Identifying** and assessing actual and potential human rights impacts
  - **Acting on and integrating** the assessment findings into a management plan for operations
  - **Tracking and monitoring performance** in managing impacts
  - **Communicating** that performance to relevant stakeholders
- Providing or cooperating **in remedying** actual impacts caused or contributed to either through the company's own grievance mechanism or other grievance mechanisms (including judicial and non-judicial mechanisms, whether state-based or non-state based)

Key Points for Human Rights Due Diligence

Companies conducting human rights due diligence in Myanmar should note that:

- Situations and operations change. Due diligence should be an on-going activity, carried out particularly before new activities or business relationships commence or the surrounding context alters. There should be continuous assessment of potential impacts during the full lifecycle of operations or a company's role in operational activities.
- Human rights due diligence should be built on a recognition that different types of activities can have quite distinct impacts on different human rights and can affect different groups, or some individuals within certain groups differently. For example, impacts can be more severe where individuals or groups are marginalised or at risk (see Chapter 4.8 on Groups at Risk in Myanmar).[44]
- The current fluidity in the national legal framework is another reason why all companies should look to international standards as an anchor for their social, human

[42] See the International Chamber of Commerce, "Guidelines for International Investment" (2012) that call on businesses to respect human rights in line with the UN Guiding Principles, pg. 18.
[43] See, European Commission, "ICT Sector Guide on Implementing the UN Guiding Principles on Business and Human Rights" (2013).
[44] To see some indicative examples of impacts on different stakeholders during different ICT activities, see: European Commission, "ICT Sector Guide on Implementing the UN Guiding Principles" (2013), pg 10.

rights and environmental due diligence. Benchmarking due diligence against national requirements is difficult, given the difficulties of obtaining copies of existing or emerging legislation, and could result in benchmarking against out-dated laws.

- Due diligence should also cover risks that business relationships pose to human rights (see Table 4 below). While all companies – international and local – operating in the sector, including suppliers, have their own standalone responsibility to respect human rights, they must also assess and address the impacts business partners cause that are directly linked to their operations, products or services.[45]

Business Relationships in the ICT Sector in Myanmar

Companies will need to carry out careful due diligence on the background, ownership, policies and practices of potential business partners, including whether they are, or have been, subject to any current or former US sanctions lists involving Myanmar.[46] As many of the larger Myanmar companies are involved in other sectors, it will be relevant to look across operations to understand how they conduct their business in those other sectors.

Finding the right business relationships in Myanmar will therefore require enhanced due diligence throughout the life of the particular relationship:

- **Before entering into the relationship:** Carry out due diligence on business partners and their policies and practices for addressing environmental, social, human rights impacts and corruption; including identifying directorships in other companies held by business partners.
- **Documenting the terms of the relationship:** Include contractual requirements on meeting relevant international standards.
- **Supporting the relationship:** Provide advice, training, and capacity building on how business partners or entities in the value chain should responsibly conduct themselves. A relationship provides the opportunity to promote better corporate governance and share policies and practices on managing environmental, social and human rights impacts.[47]
- **Monitoring the relationship:** Include requirements ranging from self-assessment and reporting, visual inspections, to third party monitoring, depending on the business relationship's level of risk.
- **Ending the relationship:** Include provisions to escalate and permit termination of the contract if for example there are findings or credible allegations of severe human rights violations or failure to take the required corrective actions.

[45] UN Guiding Principle 11, Commentary: "*The responsibility to respect human rights is a global standard of expected conduct for all business enterprises wherever they operate. It exists independently of States' abilities and/or willingness to fulfil their own human rights obligations, and does not diminish those obligations*."
[46] See: http://www.treasury.gov/ofac/downloads/prgrmlst.txt and an overview of current US sanctions: http://burma.usembassy.gov/sanctions-overview.html
[47] See, IHRB, "State of Play: The Corporate Responsibility to Respect Human Rights in Business Relationships" (Dec 2013).

1

D. SWIA Methodology

The methodology for this ICT SWIA has been developed by IHRB and DIHR in cooperation with MCRB.

Myanmar is undergoing rapid changes so companies operating in the sector will need to be well-equipped to assess and manage change. This SWIA, building on existing impact assessment and management techniques and on the UN Guiding Principles, emphasises the ongoing management of potential negative and positive impacts as well as the need to use management systems that can adapt to situations (i.e. actual impacts) that were not predicted at the design stage of a project.

Table 4: SWIA Mitigation Hierarchy

Companies should seek to address potential human rights impacts using a mitigation hierarchy:

- first anticipate potential impacts in order to **avoid or prevent** them
- where avoidance is not possible, **minimise** the impacts that occur, and finally
- **remedy** impacts that occur.

The Three Pillars of the UN Guiding Principles and SWIA Three Levels of Business Impact: Sector, Project and Cumulative

The SWIA responds to the three pillars of the UN Guiding Principles as follows:

- **Pillar I. State Duty to Protect:** This includes a detailed examination of whether Myanmar's ICT policies and laws can promote or hinder responsible business. The analysis looks in particular at whether they are aligned with relevant international human rights standards. Where they are not, it identifies the gaps.
- **Pillar II. Corporate Responsibility to Respect:** Within this Pillar, the SWIA looks at a range of operations across the ICT sector and examines the impacts of the sector at the **three levels of impacts** identified below.
  - **Sector-level:** This level of assessment considers the broader, aggregate, country-wide impacts, positive and negative, of the sector on the national economy, the country's governance and the overall environment and society. In order to be able to address the root cause of potential negative impacts, the SWIA includes an analysis of the relevant policy and legal frameworks that helps shape business conduct (where available) and the national context that businesses and civil society need to address in order to achieve more responsible business conduct. The SWIA also draws out recommendations on opportunities to improve human rights outcomes at the sectoral level. A sectoral view should help stakeholders see the 'bigger picture' of potential negative impacts of projects in a whole sector, as well as potential opportunities for positive human rights outcomes, and to make choices based on a broader perspective.
  - **Cumulative level:** Where there are numerous ICT operations in the same area, this may create cumulative impacts on surrounding society and the environment that are different and distinct from impacts of any single company or operation. Managing those impacts typically requires the government authorities to participate or take a

leading role. However, company-Government cooperation or at least company-company cooperation is also essential. The SWIA identifies potential areas or activities that may lead to cumulative impacts and identifies options for collective sectoral action to address the impacts observed in, and predicted for, Myanmar.

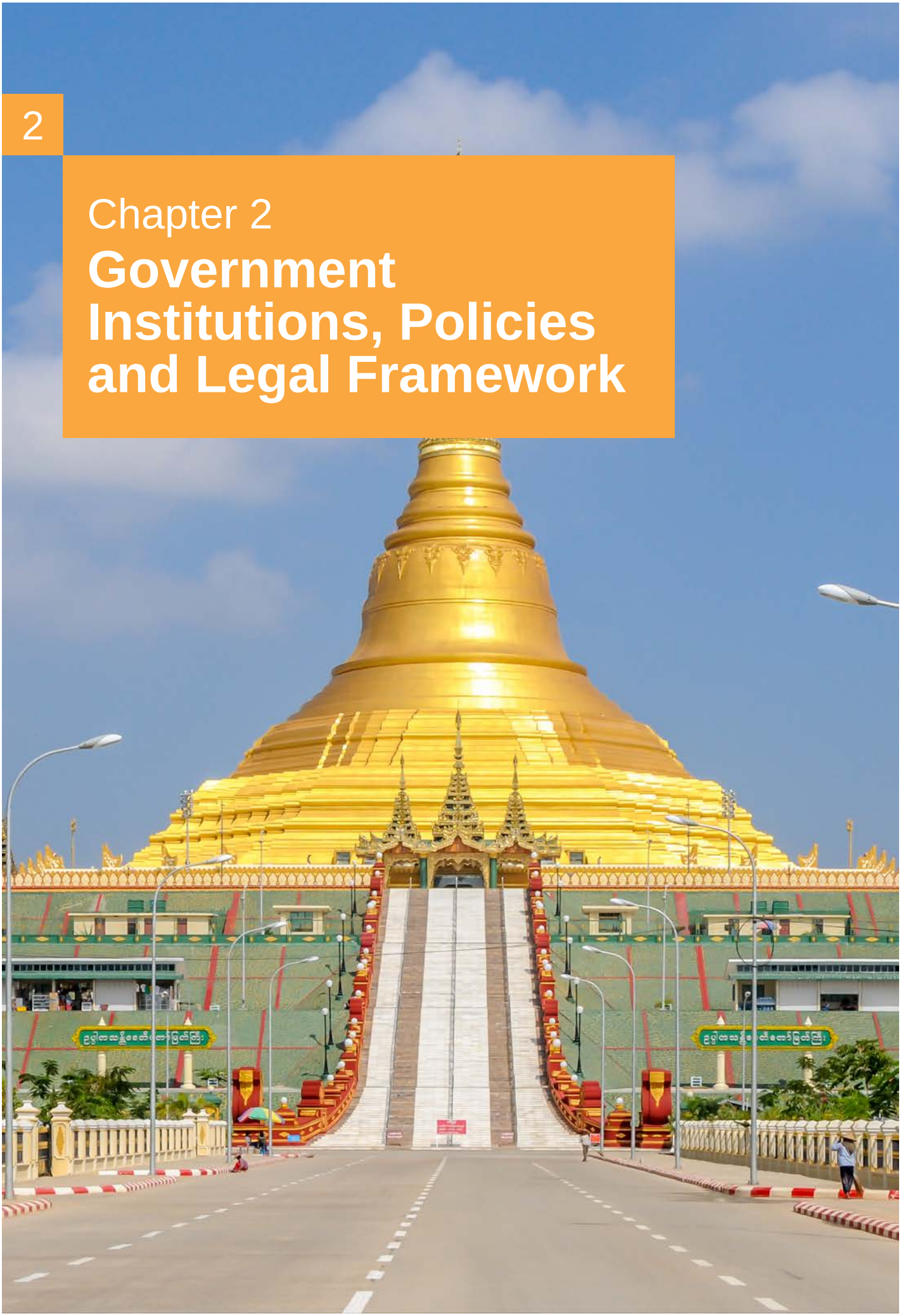
- **Operational level:** The SWIA looks across a range of existing operations in the ICT sector in Myanmar. The findings represent common operational-level impacts that are relevant to the ICT sector, recognising that impacts are often very context-specific and importantly can be avoided or shaped by (good and bad) company practices. In addition to looking at actual and potential negative impacts from operations in the sector, the SWIA also catalogues positive impacts observed in Myanmar during the SWIA desk and field research, so that stakeholders can learn from these examples.

- **Pillar III. Access to Effective Remedy:** This includes a review of the options for remedy of negative human rights impacts by companies or the Government, looking at the current ecosystem of potential judicial and non-judicial remedies available in the country.

See Annex A for a more detailed description of the SWIA methodology and the scope and coverage of the field research carried out.

2

Chapter 2
Government Institutions, Policies and Legal Framework



Chapter 2

2

ICT Government Institutions, Policies & Legal Framework

In this Chapter:

This Chapter sets out the existing Government institutions, policies and legal frameworks relevant to the ICT sector in Myanmar. The absence of clear expectations by Government as to acceptable business conduct, as set out in policies, laws or other expressions of Government expectations, results in gaps that can be filled by responsible – or irresponsible – company actions. As such, impacts often arise from a combination of Government legislation, action or policy (or lack thereof), and company action operating under or outside of the legal and policy framework. It is therefore important to understand whether the policy and legal framework actually requires responsible business conduct, or whether it even addresses relevant issues. It may even actively require businesses to violate international human rights standards in order to comply with national law.

Home governments of international companies operating in Myanmar can also play a role in setting out clear expectations of responsible business conduct.

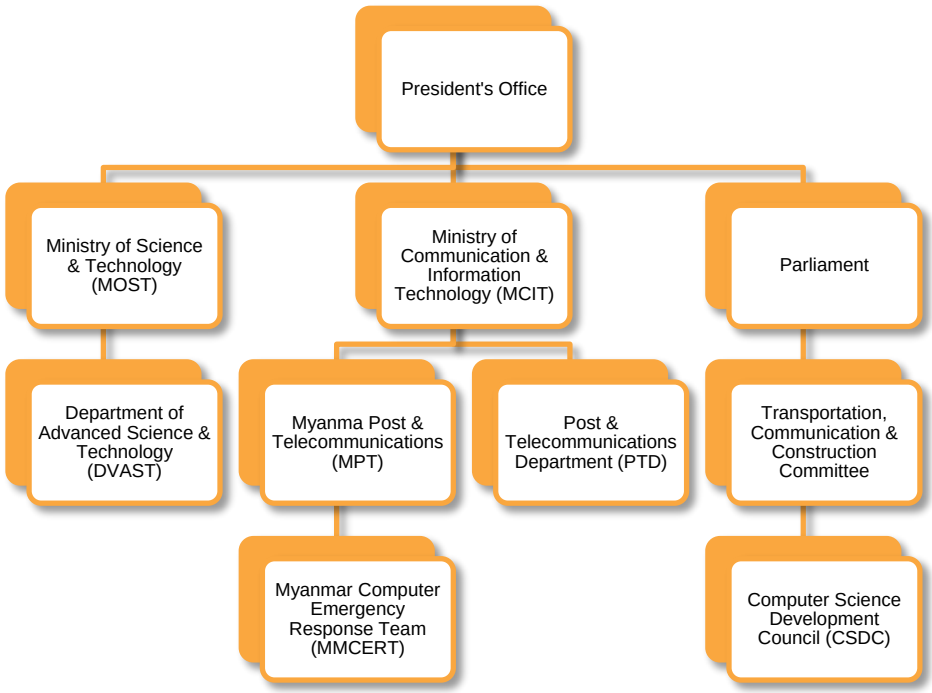
2

A. Key Actors Regulating Myanmar's ICT Sector

Government Institutions Regulating ICT Operations in Myanmar

There are a range of Government institutions involved in the governance and regulation of the ICT sector in Myanmar. The main actors and their functions are highlighted below.

Figure 1: Government Institutions Regulating ICT Operations in Myanmar



The Ministry of Communications and Information Technology (MCIT)

The Ministry of Communications and Information Technology (MCIT)[48] was formerly the Ministry of Posts and Telegrams prior to a restructuring in November 2012. MCIT is the Myanmar Government ministry mandated to guide the development of the country's ICT sector and is the lead ministry responsible for investment in the ICT sector.

MCIT led the 2013-2014 tender process for the licensing of two foreign mobile operators, and has issued the requirements and various classes of licenses available for ICT related businesses (see further Chapter 3, section B on Sector-Level Impacts). MCIT is tasked with modernising Myanmar's ICT sector, supporting on-going liberalisation for local and foreign investors, lowering service prices for customers, developing Myanmar's ICT labour force, and promoting access in underserved locations through the country.

[48] See the website of the Myanmar Ministry for Information and Communications Technology (MCIT).

Post and Telecommunications Department (PTD) and Myanma Posts and Telecommunications (MPT)

Within MCIT, there are currently two sub-divisions: the Posts and Telecommunications Department (PTD)[49] and Myanma Posts and Telecommunications (MPT).[50] Both are currently undergoing wholesale re-structuring. The draft 2015 Telecoms Master Plan outlines a restructure of Myanmar's ICT related institutional framework to create a new 'industry ecosystem'. Under the Master Plan, MCIT will be split into two regulatory bodies and two operators, so that there is independence between operations and regulation, policymaking and oversight responsibilities, including for cybersecurity. Committing to a clear legal, regulatory, and technological separation between Ministry of Communications and Information Technology (MCIT), service operators (MPT and private), and security agencies is a welcome step in the reform of the ICT sector (see further Chapter 4.3 on Privacy and Chapter 4.4 on Surveillance).

PTD is currently the ICT regulatory authority in Myanmar and manages the telecommunications licensing system and spectrum management (detailing specific technology and businesses permitted to transmit on specific radio frequencies in Myanmar). PTD is intended to become an independent regulator[51] by end 2015, to be called the Myanmar Communications Regulatory Commission (MCRC). Its core functions will reportedly be: licensing; spectrum management; interconnection; infrastructure sharing; price and access regulation; equal access and competition; and consumer rights and disputes management. ICT Security (ICTS) will be the other regulatory authority, responsible for e-government, ICT security and satellites, and will incorporate the Myanmar Computer Emergency Response Team (MMCERT), the primary national-level government entity monitoring and reporting cyber-security incidents.

Myanma Post and MPT are the two operators. MPT is a Government-owned mobile network operator and provider of fixed line Internet and voice services. As part of the World Bank's Telecommunications Sector Reform Project, it is undergoing a process of corporatisation**.** In July 2014 MPT announced a joint operations agreement with Japan's KDDI Summit Global Myanmar Co. Ltd. (KSGM). KSGM is a subsidiary of a joint venture between Japanese telecommunications operator KDDI and Sumitomo Corporation. The joint operations agreement is focused on upgrading existing telecommunications infrastructure, enhancing customer service, and reorganising business processes for MPT[52].

[49] Ibid.
[50] Ibid.
[51] See World Bank "Project Appraisal Document On a Proposed Credit in the Amount of SDR 20.60 Million ($31.5 Million Equivalent) to the Republic of the Union of Myanmar for a Telecommunications Sector Reform Project" (January 2014), p3.
[52] KDDI Corporation, "Entering the Telecommunications Business in the Republic of the Union of Myanmar" (July 2014).

Ministry of Science and Technology (MOST)

The Ministry of Science and Technology (MOST) is active in ICT human resource development in Myanmar and responsible for the management of technical and computer universities.[53] Within MOST, management of computer universities is overseen by the Department of Advanced Science and Technology (DAST). In addition to the 26 computer universities currently in existence in Myanmar, DAST also manages five technological colleges. Yangon Technological University and Mandalay Technological University are designated as "*Centres of Excellence*". Through a partnership with the Government of India, DAST also manages the India-Myanmar Centre for Enhancement of Information Technology Skills (IMCEITS) located in Yangon.

Computer Science Development Council

The Computer Science Development Council was established in 1996 by the *Computer Science Development Law* (see Section D below). The Council is responsible for developing policies related to information technology, computer networks, and computer science. The Council is chaired by the Union Minister of MCIT and plays a key role in the development of ICT policy, providing legislative inputs to the Pyithu Hluttaw Transportation, Communication and Construction Committee. The Council is comprised of various ministers and members of Government departments or organisations.[54] Civil society members are not included in the Council's membership, although it include members in its Executive Committee from the Myanmar Computer Federations (MCF) (see Table 5 below), as a channel for providing subject matter expertise during the legislative process.

Under the 1996 *Computer Science Development Law* the stated duties of the Council include:[55]

- Setting policy and giving guidance for the "*development of computer science in the State*" and the development of an ICT network
- Supervising and giving guidance with respect to activities of the Federation and other computer-related associations
- Prescribing the types of computer software and information which are not permitted to be imported or exported[56]
- Abolishing any computer association formed or existing or not functioning in conformity with the provisions of the law or the constitution of the relevant association.

Other Actors Involved in Myanmar's ICT Sector

Other Actors Involved in Myanmar's ICT Sector

There are a number of other actors and multi-stakeholder bodies relevant to Myanmar's ICT sector (some of which have been established or supported by the Myanmar

[53] See: Modins, "Government and Policy: Ministry of Science and Technology" (last accessed August 2015).
54 See the *Myanmar Computer Science Development Law* (No.3/96), section 4.
55 Ibid, section 8.
56 Ibid.

Government) and include representatives from the private sector, civil society organisations, and key development partners.

Table 5: Other Actors Involved in Myanmar's ICT Sector

The Myanmar Computer Federation (MCF) Established in 1998 as part of the *Computer Science Development Law*. MCF is an umbrella organisation made up of all the official computer-related associations and technical groups in Myanmar. The MCF performs a variety of functions including assisting in the development of ICT policy, holding technical seminars and workshops, holding ICT case study competitions, trainings, and sending delegations overseas. The MCF works closely with the Computer Science Development Council. There are various sub-associations of Myanmar Computer Federation, including the Myanmar Computer Industry Association (MCIA), Myanmar Computer Professionals Association (MCPA) and Myanmar Computer Enthusiasts Association (MCEA).
Myanmar Computer Industry Association (MCIA) The MCIA leads coordination between State and Division level computer industry associations, while working to implement the objectives in the 1996 *Computer Science Development Law*. The MCIA State and Division associations include[57]: ■ Yangon Computer Industry Association (Yangon) ■ Mandalay Computer Industry Association (Mandalay) ■ Ayeyarwaddy Computer Industry Association (Pathein) ■ Sagaing Computer Industry Association (Monywa) ■ Shan Computer Industry Association (Taunggyi) ■ Mon Computer Industry Association (Mawlamyine) ■ Bago Computer Industry Association (Bago) ■ Magway Computer Industry Association (Magway)
Myanmar Computer Professionals Association (MCPA) The MCPA functions similarly to the MCIA in terms of serving as a coordinating body between State and Division level organisations. The MCPA holds seminars related to computer science and also participates in research related to computer science and technology.
Myanmar Computer Enthusiasts Association (MCEA) Established in 1998, the MCEA includes over 100,000+ basic education student members.[58] MCEA does not currently have an independent website.

57 See, Myanmar Computer Industry Association, "Organisational Structure" (last accessed August 2015).
58 See, Myanmar Computer Federation, "MCEA" (last accessed August 2015).

ICT Sector Working Group

The ICT Sector Working Group is one of the 16 sector working groups established as a result of the Nay Pyi Taw Accord[59] between the Myanmar Government and donor governments.[60] The ICT Sector Working Group comprises development partners, the Government, the Myanmar Computer Federation (MCF), Myanmar Development Resources Institute, Myanmar ICT for Development Organisation (MIDO), and the Myanmar Centre for Responsible Business (MCRB).[61]

The ICT Sector Working Group was established to support the transformation of Myanmar's ICT sector, with a focus on developing an effective regulatory framework that "*facilitates entry of private service providers*".[62] Additional focus areas include E-governance, ICT education for all, and improving access to technology for students and workers.

ICT for Development (ICT4D) Working Group

'ICT 4 Development' (ICT4D) is a broad field including but not limited to using ICT to promote mobile health, education and agriculture. The ICT4D Working Group acts a focal point for communication and coordination between stakeholders, while also promoting common platform development and sharing of best practices. Membership in the ICT4D Working Group is open. Current members include NGOs, international donors, private sector companies, civil society organisations. The ICT4D working group is chaired by PACT, a U.S. based international NGO.[63]

For the main NGOs and CSOs working in the ICT sector see the current list of 'Linked Initiatives' on MCRB's website.

Donor Programmes: The World Bank's Telecommunications Sector Reform Programme

The World Bank's Telecommunications Sector Reform Project with the Ministry of Communications and Information (MCIT) is a $31.5 million project running from April 2014 to June 2019. The Project's primary goals are to:

> "*(a) improve the enabling environment for the telecommunications sector and extend coverage in selected remote pilot locations; and*
> *(b) establish priority eGovernment technological foundations institutional capacity for Government to embark on its public sector reform program*."[64]

59 See "Nay Pyi Taw Accord for Effective Development Cooperation" (last accessed August 2015).
60 See, Myanmar Information Management Unit, "Aid Policy and Coordination" for additional information on Government of Myanmar-Development Partner meetings (last accessed August 2015).
61 See: Sector Working Group Dashboard available from MOHINGA Resources (last accessed August 2015).
62 See "Communication and Information Technology Sector Working Group Dashboard"
63 For additional information on the ICT4D Working Group, please see "Terms of Reference"
64 See World Bank "Project Appraisal Document On a Proposed Credit in the Amount of SDR 20.60 Million (USD 31.5 Million Equivalent) to the Republic of the Union of Myanmar for a Telecommunications Sector Reform Project" (January 2014), pg v.

The primary goal of the 'enabling environment' project component is the establishment of competitive sector. To achieve this, the World Bank is providing technical assistance, policy guidance, and assistance in financing key investments such as a spectrum management and monitoring system, which will allow MCIT to designate which entities are permitted to use specific radio frequency for wireless communication and to monitor compliance. $2.2 million will be allocated to support the corporatisation of MPT and the eventual registration of MPT as a limited liability company.[65] The World Bank will also be providing "*technical assistance as needed for due diligence reviews of a suite of laws, including privacy, data protection, cyber-crime and access to and freedom of information and recommendations regarding the elaboration of legal and regulatory tools reflecting international best practice in these areas.*"[66]

In order to facilitate increased rural connectivity, the World Bank is supporting MCIT in the development of a process that would subsidise telecommunications and Internet infrastructure in areas of Myanmar that may otherwise be considered economically unviable.

The majority of the 'enabling e-government foundations' component will be devoted to developing a 'Myanmar National Portal' to provide "*citizens, businesses and visitors (including foreign workers, investors and tourists) with a single on-line window for Government information and services*".[67] The portal will reportedly be developed into a mobile friendly tool for users to find such information in the Myanmar and English languages.[68] The portal will also provide an outlet for users to provide suggestions and feedback about poor service delivery or incidents of corruption, and transact services in a safe and convenient electronic environment. This important objective of improving transparency and accountability represents a significant and welcome shift from earlier Government practices.

While a public consultation with civil society and community members was held in relation to the Telecom Sector Reform Project, it has been the subject of criticism from some civil society groups concerned that human rights considerations, particularly in terms of privacy and surveillance, have not been incorporated into project plans or priorities.[69] In addition, civil society has drawn attention to the lack of consideration of human rights risks within seemingly 'neutral' issues like equipment procurement, expressing concerns about the potential installation of equipment such as deep packet inspection can be used to detect abnormal network activity that may be evidence of a cyber-attack but can also enable the filtering of content and surveillance (see further Chapter 4.3 on Privacy and Chapter 4.4 on Surveillance).

65 Ibid, pg. 8.
66 Ibid, pg. 25.
67 World Bank, "Myanmar Moves Toward Connectivity for All" (6 February 2014).
68 See, World Bank "Project Appraisal Document On a Proposed Credit in the Amount of SDR 20.60 Million (USD 31.5 Million Equivalent) to the Republic of the Union of Myanmar for a Telecommunications Sector Reform Project" (January 2014), pg 21.
69 US Campaign for Burma et al, "Civil Society Comments on the World Bank Telecom Sector Reform Project in Burma" (21 January 2014).

2

Donor Programmes: The Asian Development Bank's support to the E-Governance Master Plan

See Section B below.

B. Policy Frameworks Guiding Myanmar's ICT Sector

The 2012–2015 Framework for Economic and Social Reform (FESR)

President Thein Sein's post-election political, economic and administrative reforms were formalised in the Government's 2012–2015 Framework for Economic and Social Reform (FESR)[70] which is meant to be a 'reform bridge' linking current reform programmes to the Government's twenty-year national development plan. The FESR identifies priority sectors and potential 'quick wins', is meant to serve as a reference in developing sectoral and regional plans, and provides a steer for development cooperation with international partners.[71]

The FESR identifies improving mobile phone and Internet services quickly "*to help people access information, create business opportunities, lower transaction costs and enhance social interaction*" as one of its important 'quick wins.' It sets an ambitious target of reaching 80% mobile phone penetration by 2015 and identifies two dimensions of policy reform that are particularly important for a rapid and successful expansion in penetration rates: first, full liberalisation of the market, including opening up to foreign as well as domestic investors; and second, creating an effective regulatory system that ensures competition among suppliers and minimises prices charged to customers.[72]

The Government's ambitious plans to upgrade its Internet infrastructure is presented as a means to allow a comprehensive e-strategy for leapfrogging in a number of areas: educational programs, Government regulation and knowledge management. The FESR highlights the on-going process of preparing a medium to long term plan for the sector (see below on the different ICT-related Master Plans) and drafting of a *Telecommunications Act* (adopted in 2013 and now in force, see below) that clearly sets out how the Government will separate the policy, regulatory and operational roles of the Government in the sector and establish an independent regulator.[73]

The FESR focuses on market liberalisation and infrastructure improvements as key drivers of increased mobile penetration and economic development. It recognises the importance of providing digital services such as mobile money, but does not acknowledge the need for security safeguards to protect users and businesses. As the ICT sector has

70 Government of Myanmar, "Framework for Economic and Social Reform - Policy Priorities for 2012-2015 towards the Long-Term Goals of the National Comprehensive Development Plan (FESR)" (January 2013).
71 Tin Maung Maung Than, "Introductory Overview: Myanmar's Economic Reforms", Journal of Southeast Asian Economies, Vol. 31, No. 2 (August 2014).
72 Government of Myanmar, "Framework for Economic and Social Reform - Policy Priorities for 2012-2015 towards the Long-Term Goals of the National Comprehensive Development Plan (FESR)" (January 2013).para. 8.
73 Ibid, para. 78.

developed, stakeholders in the financial services industry have noted that the Central Bank of Myanmar's recent mobile money licenses do not require service providers to adopt specific security standards.[74]

The FESR's operational period is shortly coming to an end in 2015. As such, it is important that the Government's other ICT policy frameworks (see below) reinforce the FESR's commitment to people-centred development by adopting clear and justifiable limits on Government involvement in and access to the ICT sector that are aligned with international standards and best practice (see Recommendations to the Government of Myanmar).

The 2011-2015 ICT Master Plan

Prior to the FESR (see above), the Government's reform commitments to liberalise the ICT sector in Myanmar were largely contained in three separate ICT Master Plans covering 2001–2005,[75] 2006–2010,[76] and 2011–2015. None of the Master Plans were developed or issued by the MCIT or the Government more generally. As a result, many of the objectives lack a clear strategy for robust implementation or enforcement. Instead, the Myanmar Computer Federation (MCF) developed the most recent 2011-2015 ICT Master Plan with support from the Korean International Cooperation Agency and the Electronics and Telecommunications Research Institute (a government supported research institute in Korea). A full version of the Master Plan is not currently available online – only a PowerPoint file providing an overview, rather than the Master Plan itself – meaning specific details as to each of the four functional areas of focus are not publicly available.

The 2011–2015 ICT Master Plan adopts key objectives across four functional areas covering: infrastructure, ICT Industry, ICT Human Resource Development (HRD) and E-education (see Table 6). It sets out various ambitious objectives that are positive from a human rights and social development perspective, including the creation of a research and development centre for ICT security, establishing national software institutes and ICT teacher training programs, and providing Internet access to 1,000 high schools.

The results of the 2011-2015 Master Plan have been mixed, at least in part due to the fact that the Master Plan has not been adopted or enforced as an official Government policy framework. While various objectives such as growing total subscribers (to 30 million by 2015), increasing tele-density (the number of telephone subscriptions per 100 inhabitants) to 50% by 2015[77] and licensing private operators in the telecommunications sector have been realised, a number of objectives have not yet been achieved. These include (but are not limited to) promoting Myanmar as an ICT outsourcing destination globally, the majority of the stated e-education initiatives and developing a *Cyber Information Act*. In addition, the 2011–2015 ICT Master Plan did not address gaps in the legal framework governing

[74] See Myanmar Times, "Preparing the Financial System for Digital Attacks", (March 2015).
75 Prepared by the Myanmar Computer Federation (MCF).
76 Prepared by the MCF and Republic of Korea under the Initiative for ASEAN Integration.
77 MCIT noted that 50% mobile penetration (28.1 million SIM cards) was achieved as of June 2015. See: Myanmar Times, "Mobile Penetration Reaches Half the Country" (June 2015).

2

ICT operations (specifically concerning intellectual property, freedom of information, lawful interception or data privacy and protection).

Table 6: ICT Master Plan 2011–2015 Action Items across 4 Key ICT Sector Areas

ICT Infrastructure (*INF*)	ICT Industry (*In*)	ICT Human Resource Development (*HR*)	E-education (*Ee*)
INF1: Demand Path Estimation for ICT Infrastructure Expansion	*In1*: Develop promotion policies for ICT SMEs and venture businesses	*HR1*: Develop the ICT network for University	*Ee1*: Establishment of national committee for information culture movement
INF2: R&D Centre for ICT Security	*In2*: Give support for the firms in the ICT industry zone	*HR2*: Set up model schools for ICT (software institutes)	*Ee2*: Production and distribution of the booklets for promoting information culture
INF3: Tariff Policy	*In3*: Establish ICT research centre	*HR3*:Industry University cooperation program for training & R&D collaborations	*Ee3*: Refresh laws and rules for acceleration of e-Awareness
INF4: Network Migration Roadmap	*In4*: Enlarge R&D investment and facilities	*HR4*: Set up a National Research Centre/HRD centre for ICT development	*Ee4*: Incorporation of ICT training into school curriculum
INF5: Proactive ICT Infrastructure Construction	*In5*: Increase outsourcing demand of public sector	*HR5*: Establish and international cooperation network between Myanmar and Foreign ICT University	*Ee5*: ICT teacher training program
I*NF6*: Promotion of ICT HRD for professional	*In6*: Develop ICT support tax system	*HR6*: Set up national certification	Ee6: Development of textbook and contents for ICT training
INF7: Public protection and disaster relief	*In7*: Expedite market opening and promote international relationship	*HR7*: Set up digital libraries that connect all other universities	*Ee7*: Distribution of ICT textbook and contents
INF8: Establishment of a network management centre		*HR8*: Regional positioning activities as S/W and ICT services outsourcing centre for neighbouring countries	*Ee8*: Refresh Laws and rules for promotion of digital literacy
INF9: ICT standardisation for the protection of local Industry & expansion of business opportunity		*HR9*: Incentive policy to foster research personnel	*Ee9*: National LAN installation and Internet connections for 1000 high schools
INF10: restructure of network service provider (operation and			

maintenance)		

Source: MCIT, KOICA, ETRI, "The Follow-Up Project of the Myanmar ICT Master Plan," (2011)

The Telecommunications Master Plan

On 14 May 2015, MCIT hosted an initial consultation on "*Creating a Master Plan for Myanmar Telecommunications*" in Nay Pyi Taw. The proposed Master Plan outline covered rural and regional development, roles and responsibilities of MCIT, PTD, other Government bodies and MPT and other operators, as well as key topics forming a 'reference framework', including Net Neutrality (the principle of treating Internet traffic and content delivery in a neutral manner, without throttling or preferentially accelerating access), universal service, and privacy and security.

Table 7: Proposed Vision of the 2015 Draft Telecommunications Master Plan, as of August 2015

The draft Master Plan sets out three broad goals:

- to create a Myanmar national broadband infrastructure with affordable services
- to deliver communications content and services for the Myanmar people in a rights-respecting, mobile-first system
- to develop an institutional and policy framework for effective oversight

Source: Draft Telecommunications Master Plan 2015

In late July 2015, a draft Telecommunications Master Plan was published for public consultation through 7 August 2015 (Table 7).[78] Several organisations, including the Myanmar Centre for Responsible Business (MCRB), MIDO and Access (a US based digital rights organisation), provided comments on the draft Masterplan.[79] Both MCRB and Access called for:

- A commitment not to shut down communications networks, as the Myanmar Government did in 2007 (See Chapter 4.1 on Freedom of Expression)
- The release of 'transparency reports' by Myanmar's regulatory bodies to provide the public with information about Government access to user data (See 4.4 on Surveillance) and by telecommunication companies (noting that Telenor has already done this)
- A data protection system that informs and protects users, while also encouraging innovation (See Chapter 4.5 on Cybersecurity)
- A lawful intercept framework including access to remedy (see the Annex to the Recommendations)
- A commitment to Net Neutrality, which is fundamental to ensure that the Internet remains a platform for the enjoyment of human rights and innovation

[78] Myanmar Ministry of Communications and Information Technology, "Draft Telecommunications Masterplan" (8 July 2015).
[79] MCRB, "Comments on the draft Myanmar Telecommunications Master Plan" (30 July 2015).

When delivering services to the Myanmar people, MCRB recommended that services should be widely available in Burmese and also in ethnic languages in the ethnic regions. In addition, MCRB highlighted that time should be given to ensure local level stakeholder engagement and communication with regards to building towers and laying fibre, and requiring and enforcing adequate health and safety protection for workers involved (See Chapter 4.6 on Labour and Chapter 4.7 on Land).

The E-Governance Master Plan

Myanmar is currently developing an E-Governance Master Plan 2015 with support from the Asian Development Bank (ADB)[80]. The Government is focusing on streamlining its processes to improve efficiency through the development of a common framework for ICTs, transparency and a wider reach of public service delivery. The Master Plan will guide continuous and more detailed planning in the areas covered. For example, the Master Plan lays out a conceptual architecture for cybersecurity, while the detailed operationalisation will be developed to meet the needs and specific characteristics of evolving e-governance interventions.

A draft E-Governance Master Plan shared with the ICT Sector Working Group focuses on the use of ICTs in the reform of public-sector processes to implement a coherent and systematic approach to the design, evaluation and adoption of the systems underpinning public services to improve their delivery and efficiency. Out of a total of 21 Government Ministries, only nine are included in the draft Master Plan.[81] Process reform is intended to be supported by common infrastructure and shared software applications among the nine participating Ministries.

The common shared software being used across these ministries is intended to focus on areas that will improve operational efficiency and communication within the Government, including email, human resources management and payroll, and e-office tools. Under the E-Governance Master Plan, the MCIT is also tasked with developing a 'citizen service centre'. It is unclear if this task overlaps with the Myanmar National Portal (to provide accessible public information on Government services) being developed under the World Bank's Telecommunications Sector Reform Project (see section A above)[82] and what

80 ADB, "Project 47158-001: Design of e-Governance Master Plan and Review of Information and Communication Technology Capacity in Academic Institutions" (2013)

81 Participating ministries include the: Ministry of Communications and Information Technology, Ministry of Construction, Ministry of Power, Ministry of NPED, Ministry of Commerce, Ministry of Transport, Ministry of Home Affair, Ministry of Rail Transport. It is unclear why these ministries, and not others (or all), are participating.

82 The World Bank's Telecommunications Sector Reform project calls for the development of "*A mobile friendly Myanmar National Portal ($ 3.62 million) will be financed to provide citizens, businesses, and visitors (comprising of foreign workers, investors and tourists) with a single window into the information and services offered by the Government. Over time the National Portal will allow its users to find relevant information, provide suggestions and feedback, and transact services in a safe and convenient electronic environment*."

services would be offered through the citizen service centre beyond e-payments from citizens to Government. [83]

It is currently unclear how protection of the right to privacy will be incorporated into the Master Plan's design, any implementation of e-Governance practices within Government apparatus, or any future e-Government related regulations. User trust is central to the concept of ICTs and e-Governance. If people and businesses do not believe that their personal data will be safe and secure from unwarranted surveillance or misuse, then they will be less likely to use e-Government and other services. This could undermine the Master Plan's ability to support accountability, transparency and progress in human rights and social development in Myanmar. [84] (See further Chapter 4.3 on Privacy and the Recommendations to the Myanmar Government).

Regional Policy Frameworks: The 2015 ASEAN ICT Master Plan

The 2015 ASEAN ICT Masterplan was developed by Government Ministers, policy makers, regulators and the ICT industry within the ASEAN region. It focuses on three pillars – economic transformation, people empowerment and engagement – supported by a foundation of infrastructure development, bridging the digital divide and human capital development.[85] Recognising the key transformational role that ICT can play in promoting economic development and integration, it is also acknowledges and encourages the role of ICT in building more empowered and inclusive societies "*involving all the stakeholders in ASEAN – government, citizens and businesses, developed and developing, rural and urban, young and old, as well as those with and without disabilities*". The Master Plan is to be implemented over the next five years.

While stakeholder consultations highlighted the need for more transparency,[86] the Master Plan does not address the role of ICT in improving transparency and accountability, nor does it address the sector's important role in promoting freedom of speech. The Master Plan will therefore will provide little guidance to the Government of Myanmar in finding the appropriate balance in improving accountability, transparency and the protection of human rights in developing its regulatory framework.

[83] See: ADB, "Myanmar: Design of e-Governance Master Plan and Review of Information and Communication Technology Capacity in Academic Institutions" (last accessed August 2015).
84 US Campaign for Burma et al, "Civil Society Comments on the World Bank Telecom Sector Reform Project in Burma" (21 January 2014), p. 3.
85 ASEAN, "ASEAN ICT Masterplan 2015" (2011).
86 Ibid, pg. 10.

2

C. International Legal Framework Relevant to Myanmar's ICT Sector

Until very recently, Myanmar had acceded to relatively few international human rights treaties.

Table 8: Myanmar's Accession to International Human Rights Instruments

Myanmar has acceded to:

- International Covenant on Economic, Social and Cultural Rights (ICESCR) (signed July 2015)
- Convention on the Elimination of Discrimination Against Women (CEDAW)
- Convention on the Rights of Persons with Disabilities (CRPD)
- Convention on the Rights of the Child (CRC) & the Optional Protocol on the Rights of the Child on the Sale of Children, Child Prostitution and Child Pornography
- Three of the eight ILO Fundamental Conventions:
  - Forced Labour Convention (ILO Convention 29)
  - Freedom of Association and Protection of the Right to Organise
  - Convention (ILO Convention 87)
- Worst Forms of Child Labour Convention, No 182 (entered into force December 2014)
- Nineteen of the 177 Technical Conventions of the ILO, including the ILO Hours of Work (Industry) Convention
- Convention against Transnational Organised Crime, and its supplementary Protocol to Prevent, Suppress and Punish Trafficking in Persons, Especially Women and Children and Protocol against the Smuggling of Migrants by Land, Sea and Air
- UN Convention against Corruption
- Geneva Conventions I-IV
- Convention on the Prevention and Punishment of the Crime of Genocide
- UN Convention for the Safeguarding of the Intangible Cultural Heritage

Myanmar has not signed:

- International Covenant on Civil and Political Rights (ICCPR)
- International Convention on the Elimination of All Forms of Racial Discrimination (CERD)
- Convention Against Torture and Other Cruel, Inhuman and Degrading Treatment (CAT)
- Convention on the Protection of the Rights of All Migrant Workers and Members of Their Families (ICRMW)
- International Convention for the Protection of All Persons from Enforced Disappearance (CED)
- Optional Protocol to the Convention on the Elimination of Discrimination against Women (OP-CEDAW)
- Optional Protocol to the Convention on the Rights of the Child on the

involvement of children in armed conflicts (OP-CRC-AC)
- Optional Protocol to the Convention on the Rights of Persons with Disabilities(CRPD-OP)
- Five of the eight ILO Fundamental Conventions:[87]
  - Right to Organise and Collective Bargaining Convention No. 98
  - Equal Remuneration Convention No. 100
  - Abolition of Forced Labour Convention No. 105
  - Discrimination (Employment and Occupation) Convention No. 111
  - Minimum Age Convention, 1973 (No. 138)
- 158 out of the 177 ILO Technical Conventions
- Any of the four ILO Governance Conventions

In addition, the Government reportedly has not conducted any assessment of the compatibility of its existing laws with its obligations under international law.[88] Domestic courts cannot directly invoke the provisions of international or regional human rights instruments to interpret national laws unless such standards are incorporated into national legislation.[89] While it is not unusual for international law not to be automatically incorporated into domestic law, one implication of this is that Myanmar's judiciary cannot have recourse to international human rights law to circumscribe the wide discretionary powers that Myanmar's laws confer on the executive branch.

D. Domestic Legal Framework Governing Myanmar's ICT Sector

This section analyses the ICT-specific Myanmar laws in Table 9, and how the interpretation of their provisions could result in negative impacts on human rights. It should not, however, be taken as a description of how these provisions have been used in practice. That said, many of the pre-2011 laws have been used to jail political activists and human rights defenders.

It explains how even provisions identified in more recent laws might perversely require ICT companies to assist the Government to arbitrarily restrict certain rights, in order to maintain their legal licenses. Table 21 at the end of this Chapter also identifies key provisions of concern from other domestic laws not specific to ICTs that could be, and in some cases have been, used to infringe the rights to freedom of expression or association.

[87] ILO Normlex, "Up-to-date Conventions not ratified by Myanmar" (last accessed August 2015).
[88] DLA Piper et al, Myanmar Rule of Law Assessment (March 2013), p. 27.
[89] UN General Assembly, "Compilation prepared by the Office of the High Commissioner for Human Rights in accordance with paragraph 15 (b) of the annex to Human Rights Council resolution 5/1, Myanmar", A/HRC/WG.6/10/MMR/2 (15 Nov 2010), para. 5.

Table 9: Principal Existing Domestic Laws Relevant to ICTs

ICT-specific Domestic Laws:

- Telecommunications Law (2013)
- Electronic Transactions Law (2004)
- Computer Science Development Law (1996)

Laws Related to Freedom of Association Relevant to the Use of ICTs:

- Law Relating to the Registration of Organisations (2014)
- Unlawful Associations Act (1908)

Other Domestic Laws at Risk of Infringing Human Rights Relevant to the Use of ICTs:

- Emergency Provisions Act (1950)
- Official Secrets Act (1923)
- Myanmar Constitution (2008)
- Penal Code of Burma (1957)

Table 10: Existing Gaps in Myanmar's ICT Legal Framework

There are a number of substantive areas currently unaddressed under Myanmar laws or regulations. These represent major gaps in the protection of Myanmar people, ICT users and ICT companies. They include:

- Data Privacy
- Data Protection
- Access to Information
- Cybercrime
- Lawful Interception
- Intellectual Property

Table 11: Summary of Human Rights at Risk under Domestic ICT Laws

	Freedom of Expression	Right to Privacy	Equality of Access
Telecommunications Law (2013)	– Criminalisation of legitimate expression: *s68(a) & (b)* and *s66(c) & (d)* – Arbitrary blocking or filtering of content: *s77* – Arbitrary disruption or disconnection of Internet access: *s77*	– Government monitoring and surveillance of user activity and content: *s77 & s78* – Government access to user-identifying data and the right to anonymity: *s75 & s77*	– Equality of Access to information and benefits of ICTs for the rural poor, and ethnic, cultural and religious minorities: *s55*

Electronic Transactions Act (2004)	– 7-15y imprisonment and/or fines for using technology to do acts detrimental to "*state security*" or "*community peace and tranquillity*" and other vague and undefined terms: *s33(1) & (b)* – 5y imprisonment and/or fines for creating, modifying or distributing information detrimental "*to the interest of or to lower the dignity of any organisation or any person*": *s34(d)*	– Broad powers granted to a "*Control Board*" able to access and inspect any ICT it has "*reasonable cause*" to suspect was involved in an offence under the Act: *Ch. V.9*	
Computer Science Development Law (1996)	– 7-15y imprisonment for anyone using a computer or network to engage in "*any act*" which undermines e.g. "*state security*" or "*community peace and tranquillity*" and other vague and undefined terms: *s35*		

2013 Telecommunications Law

Background, Scope and Objectives

The recent *Telecommunications Law* (No. 31/2013) was adopted in October 2013, revoking the 1885 *Myanmar Telegraph Act* and 1934 *Myanmar Wireless Telegraphy Act*.[90] It also reportedly replaces the Wide Area Network Order (No. 3/2002).

Objectives of the 2013 *Telecommunications Law* include:[91]

- Supporting the modernisation and development of the nation with telecommunications technology
- Enabling telecommunications services that will be able to provide high quality and worthy (sic) services to users by allowing fair and transparent competition from domestic and abroad in the telecommunications sector which is developing
- Giving more opportunities to the general public to use the telecommunications service by expanding the telecommunications network in the entire country along with the telecommunications technology which is developing
- Protecting telecommunications service providers and users in accord with the law, including through consumer protection standards

90 See DFDL unofficial translation of *Myanmar Telecommunications Law* (No. 31/2013).
91 See Section 4, *Myanmar Telecommunications Law* (No. 31/2013)

- Supervising telecommunications service, network facilities and telecommunications equipment which require license for national peace and tranquility and for public security

The 2013 *Telecommunications Law* outlines the duties and rights of both telecommunications service providers and regulators, and sets out at high level the licensing regime for the provision of certain telecommunications services, including:

- the provision or operation of infrastructure or network facilities
- the provision of service for transmission and reception of information
- the provision of services by way of transmitting and receiving

See Table 25 in Chapter 3 for the specific types of licenses that have subsequently been issued.

Risks to the Right to Freedom of Expression

Risks related to the violation of freedom of opinion and expression under the 2013 *Telecommunications Law* can be categorised into at least three areas of concern:

- criminalisation of legitimate online expression;
- arbitrary blocking or filtering of content, and;
- arbitrary disruption and disconnection of Internet access.

These are considered in more detail below.

Criminalisation of legitimate expression online

The 2013 *Telecommunications Law* maintains some of the troubling provisions of the laws it replaces. Punishable offenses include using a telecommunications network to "*to extort, threaten, obstruct, defame, disturb, inappropriately influence or intimidate*". These are vague terms that are not defined in the Law. This creates a clear risk that the Myanmar Government could use the 2013 *Telecommunications Law* to arbitrarily characterise legitimate expression as "*threats*" or an "*inappropriate influence*", punishable as a criminal offense (see Table 12 below).

Table 12: Provisions of the 2013 Telecommunications Law with Potential to be used to Criminalise Legitimate Expression

- Content-related offenses punishable by up to 3 years' imprisonment and/or fines include "*using a telecommunications network to steal money and property, cheat and embezzle or harming the interests*" [sic] (s66(c)), or "*to extort, threaten, obstruct, defame, disturb, inappropriately influence or intimidate*." (s66(d))
- Content-related offenses punishable by up to one years' imprisonment and/or fines include "*connecting, receiving, transmitting, distributing or handing out false information dishonestly*" (s68(a)) or "*unauthorised prohibition, forbidding obstruction to the transmitting, receiving, communication, handing out or distribution of information*." [sic] (s68(b))

In addition to the risk that an end user's exercise of legitimate expression or opinion will be criminalised, ICT companies – telecommunications companies, network service providers, online publishing platforms, amongst others – may also be at risk of facilitating the allegedly criminal conduct by its users on their networks or platforms. Government-issued telecommunications service licenses are required for any entity to become a service provider (s5). Licensees are subject to suspension or termination of licenses for failure to comply with a broad set of conditions, which can include requests from Government concerning the blockage or restriction of content deemed criminal (s57). This could create a perverse incentive for ICT companies to contribute to the arbitrary criminalisation of legitimate expression in order to maintain their legal license to operate. In particular:

- The definition of "*network service provider*" includes any "*service for carrying information two ways by any means of tele-communication*" [s3(h)], meaning ICT companies are subject to these licensing risks.
- Even if the companies are not explicitly mentioned in relevant laws, language referring to the "*distribution*" or "*dissemination*" of prohibited speech could be construed as "*abetting*" the allegedly criminal behaviour, and subject to the same punishment (s73).
- The provision prohibiting "*connecting, receiving, transmitting, distributing or handing out false information dishonestly*" may also implicate ICT companies transmitting content (s68(a)).
- In general, the above provisions could also be used to compel ICT company to comply with Government requests to arbitrarily block or filter user content (see below).

Arbitrary blocking or filtering of content

The 2013 *Telecommunications Law* also provides legal capacity for the Myanmar Government to potentially block or filter user content selectively and arbitrarily (see Table 13). The law enables the Government, without clear oversight, to "*prohibit a specific type of communication*," if doing so is "*in the interest of the public*" – a very broadly worded and vague standard.

Table 13: Provisions of the 2013 Telecommunications Law with Potential to be used to Arbitrarily Block or Filter User Content

- The Government may, "*when the situation arises to carry out in the interest of the public, with the approval of the government, direct the licensee to suspend the telecommunications service provider business, prohibit a specific type of communication, to block and hold [and] to temporarily control and use the telecommunications service provider businesses and telecommunications equipment*." (s77)

As above, because licensees are subject to suspension or termination of licenses (s5) for failure to comply with a broad set of conditions (s57), there may be strong incentive for ICT companies to take action to block or filter content to avoid revocation of their license, creating a risk of contributing to Government actions in violation of freedom of expression and opinion. In particular:

- Licensees must "*make necessary preparations to enable a telecommunication service to be utilised for security matters in accordance with the law*." (s78) While this section appears to primarily justify network disconnection/suspension, it could be used to block whole websites.
- In general, the provisions cited above regarding ICT company facilitation of allegedly criminal expression may also be used to compel the ICT company to arbitrarily block or filter user content in order to avoid revocation of their license.

Arbitrary Disruption or Disconnection of Internet Access

In a world in which services such as government, health and education, are increasingly on-line and digitised, users' exercise of a wide range of human rights is tied to access to ICTs. In the case of a total network shutdown, these rights may be denied altogether.

Furthermore, in the context of a violent crackdown or other crisis, failure to broadcast news and images domestically and internationally could exacerbate violations of civil and political rights by allowing them to take place behind closed doors. During the violent crackdown against protestors in 2007 (the 'Saffron Revolution'), the Myanmar Government suspended Internet services, among other actions.

The 2013 Telecommunications Law allows for the Government to suspend or take control of telecommunications services (Table 14), but the situations in which the Government can exercise this power are unclear under the Law. The Government has not made any public commitments regarding network shutdowns during the forthcoming November 2015 elections.

Table 14: Provisions of the 2013 Telecommunications Law with Potential to be used to Arbitrarily Disrupt or Disconnect Internet Access

- Explicitly allows the Government to "*when the situation arises to carry out in the interest of the public, with the approval of the government, direct the licensee to suspend the telecommunications service provider business, prohibit a specific type of communication, to block and hold [and] to temporarily control and use the telecommunications service provider businesses and telecommunications equipment*" (s77).

Again, the *2013 Telecommunications Law* puts ICT service companies at risk of contributing to Government measures to arbitrarily disrupt or disconnect Internet access, due to the threat of their legal licence to operate (s5) being revoked for failure to comply (s57). In particular:

- In order to comply with s77 (Table 14), "*[t]he licensee shall … make necessary preparations to enable a telecommunication service to be utilised for security matters in accordance with the law*." (s78)

Risks to the Right to Privacy

Section 69 of the 2013 *Telecommunications Law* requires a court order for the disclosure of information kept in secured or encrypted systems. However the Myanmar Government has yet to draft implementing regulations governing the interception of communications by law enforcement authorities.

The Government has expansive powers under the 2013 *Telecommunications Law* to, for example, "*enter and inspect*" telecommunication services when "*in the public interest*" or "*intercept*" communications when an "*emergency situation*" arises. Implementing regulations are therefore necessary to provide clarity on the appropriate restrictions and procedures for the exercise of that power. The Annex to the Recommendations of this SWIA provides guidance on a rights-respecting framework for lawful interception that sets out the kind of restrictions on that power of interception that the Government should take into account in drafting its framework.

Risks related to the violation of the right to privacy under *the 2013 Telecommunications Law* cover two closely related areas of concern:

- Government monitoring and surveillance of user activity and content, and;
- Government access to user-identifying information and the implications for emerging international norms around the right to anonymity.

Government monitoring and surveillance of user activity and content

The Myanmar Government has a long history of close surveillance of its people. Despite ongoing reforms, the 2013 *Telecommunications Law* maintains a legal basis for monitoring communications and content. While the justification for surveillance is "*security matters*", the risk of arbitrary and / or overly broad interpretation of that provision is high (see Table 15 below).

Table 15: Provisions of the 2013 Telecommunications Law with Potential to be used to Monitor User Activity and Content

- The Government may, "*when the situation arises to carry out in the interest of the public, with the approval of the government, direct the licensee … to retrieve necessary information and communications [and] to temporarily control and use the telecommunications service provider businesses and telecommunications equipment*." (s77)

Risks of Company Involvement in Human Rights Violations

Implementing regulations of the 2013 *Telecommunications Law*, once available, may provide more guidance on the scope of expected ICT company cooperation with Government-ordered surveillance of ICT users. Currently, the *Telecommunications Law* as written leaves ICT companies open to significant risk of involvement in Government surveillance activities in a way which does not meet international standards of human rights protection.

Again, since Government-issued telecommunications service licenses are required for any entity to become a service provider (s5), licensees are subject to suspension or termination of licenses for failure to comply with a broad set of conditions (s57). This can include surveillance, and could therefore create perverse incentives for ICT companies to contribute to the arbitrary monitoring and surveillance of user activity by the Myanmar Government in order to maintain their legal license to operate. In particular:

- Government authorities, "*for defense and security matters of the State or for the public interest, if necessary … may enter into the premises of the licensed telecommunication services provider and inspect, supervise and request the licensee to submit records regarding the services.*" (s76)
- The *Telecommunications Law* also provides explicit Government authorisation "*to retrieve necessary information and communications [and] to temporarily control and use the telecommunications service provider businesses and telecommunications equipment.*" (s77)
- Accordingly, licensees must "*make necessary preparations to enable a telecommunication service to be utilised for security matters in accordance with the law.*" (s78)

Government access to user-identifying information and implications for the right to anonymity

There is a growing international concern among human rights observers about government policies throughout the world which can compromise the ability of individuals to express themselves anonymously on the Internet. The provisions of the *2013 Telecommunications Law* could be used to override anonymity, and may constitute a separate basis for violation of the right to privacy (Table 16). This may risk further undermining confidence and security on the Internet, impeding the free flow of information and ideas online.

Table 16: Provisions of the 2013 Telecommunications Law with Potential to be used to Grant Government Access to User-Identifying Information

- In order "*[t]o obtain any information or communications that may adversely affect the security of the State, the rule of law and order, the Union Government may direct the relevant organisations as necessary without infringing upon the original rights of the citizens.*" (s75)
- The Government may also, "*when the situation arises to carry out in the interest of the public, with the approval of the government, direct the licensee to… to retrieve necessary information and communications [and] to temporarily control and use the telecommunications service provider businesses and telecommunications equipment*." (s77)

Risks of Company Involvement in Human Rights Violations

Where ICT companies comply with unreasonable, overbroad, or otherwise questionable Government requests for user data under Myanmar law, they may be involved in

threatening anonymous expression and privacy online. As above, since Government-issued telecommunications service licenses are required for any entity to become a service provider (s5), licensees are subject to suspension or termination of licenses for failure to comply with Government requests to access user-identifying information (s57). In particular:

- Licensees must "*make necessary preparations to enable a telecommunication service to be utilised for security matters in accordance with the law.*" (s78)
- Moreover, Government authorities, "*for defense and security matters of the State or for the public interest, if necessary … may enter into the premises of the licensed telecommunication services provider and inspect, supervise and request the licensee to submit records regarding the services.*" (s76)

Positive Aspects on Promoting Equality of Access to ICTs

Under the 2013 *Telecommunications Law* Myanmar Ministries may create programmes for extending services to underserved areas of the country. The Myanmar Government has shown readiness in practice to achieve equality of access to ICTs (see further Chapter 3 on Sector-Level Impacts). For example:

- President Thein Sein publicly noted the importance of strengthening telecommunications access in rural areas.[92] In response, Ministry officials announced a plan to allow purchase of SIM cards in installments, with the stated aim of encouraging access for rural citizens[93]. (The need for this was subsequently overtaken by the introduction of competition in the market which led SIM Card prices to fall from 150,000 MMK to 1,500 MMK).
- In March 2015 Myanmar joined the Alliance for Affordable Internet (AFAI).[94] AFAI's goal is to realise the "*UN Broadband Commission's target of entry-level broadband priced at less than 5% of monthly income*".[95]
- In addition, each telecommunications Operator Licence includes the requirement that after three years (assuming network rollout targets are met), the operator must contribute 2% of annual revenue to a Universal Service Fund managed by MCIT that is intended to subsidise the cost of telecommunications service in areas where infrastructure deployment is not economically viable for network operators.

[92] See: The Republic of the Union of Myanmar President's Office, "Speeces and Remarks" (last accessed August 2015).
[93] Myanmar Times, "SIMs for sale by instalment in rural areas, says MPT" (8 October 2012).
[94] An ICT sector coalition that focuses on combining advocacy, research, and knowledge sharing to influence broadband policy.
[95] Alliance for Affordable Internet, "Vision and Strategy" (last accessed August 2015).

2 Electronic Transactions Law (2004)

Background, Scope and Objectives

With support from the Myanmar Computer Federation (MCF) and technical assistance from the World Bank, MCIT is in the process of reviewing the 2004 *Electronic Transactions Law*.[96] A draft of the revised law is not publicly available and there are no indications as to whether there will be public consultation on any future draft.

The 2004 *Electronic Transactions Law* as currently drafted focuses on the authenticity of electronic data as well as electronic contracts. The law also establishes a Control Board and licensing process for certification authorities in Myanmar able to issue digital certificates used to authenticate electronic communications. When information is exchanged securely online, digital certificates provide information that is used to verify the sender and recipient's identity. Under s34(a) the law criminalises hacking and unauthorised interception of communications.[97]

A draft "*Cyber-Security Law"* is also reportedly in preparation, although it is unclear if the Ministry of Home Affairs or MCIT will support MCF in drafting. (See further Chapter 4.5)

Risks to the Right to Freedom of Expression and Privacy

Though reportedly on the verge of revision, the 2004 *Electronic Transactions Law* has been used to restrict online speech deemed to be "*detrimental to the security of the state*" or "*community peace and tranquillity*", amongst other vague and undefined terms (Table 17). Between 2007 and 2009 several journalists and online activists were sentenced to long prison terms under this law, though have all since been released and it has not been used since 2011.[98]

Table 17: Provisions of the Electronic Transaction Law with Potential to be used to Infringe Freedom of Expression and Privacy

- Anyone "*using electronic transactions technology*" to do "*any act detrimental to the security of the State or prevalence of law and order or community peace and tranquility or national solidarity or national economy or national culture*," or engage in "*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 tranquility or national solidarity or national economy or national culture*," may be imprisoned for 7-15 years and/or fined. (s33(a)-(b))
- Anyone found "*creating, modifying or altering of information or distributing of*

[96] *Myanmar Electronic Transactions Law* (2004). In January 2013, lawmaker Thein Nyunt from the New National Democracy Party proposed a bill that would abolish the law, but it was rejected by the lower house. Instead he decided to amend it, and a bill to amend the law was submitted August 21, 2013 for consideration. A committee to create the new draft includes parliamentarians, NGOs, industry organizations, and others. See Radio Free Asia, "Myanmar's Parliament Considers Amending Draconian Law" (21 August 2013).
[97] See *The Electronic Transactions Law* (No. 5/2004), Art. 34(a).
[98] Specifically, Hla Hla Win, Myint Naing, Ngwe Soe (Tun Kyaw), Nay Phone Latt, Maung Thura (Zarganar), Kaung Myat Hlaing (Nat Soe), Win Maw, and Zaw Thet Htwe were imprisoned under the Electronic Transactions Act, and were all released between 2011 and 2012.

information created, modified or altered by electronic technology to be detrimental to the interest of or to lower the dignity of any organisation or any person" may be imprisoned for 5 years and/or fined. (s34(d))

- *Chapter V Formation of the Electronic Transactions Control Board and Functions and Powers thereof*
  9. The Central Body:
  (i) having access to and inspecting and checking the operation of any computer system and any associated apparatus or material which it has reasonable cause to suspect is or has been in use in connection with any offence under this Law;
  (j) exposing and acquiring any necessary identification document from any person with respect to any offence contained in this Law;

Risks of Company Involvement in Human Rights Violations

ICT companies could be implicated in assisting alleged criminal offences under the *Electronic Transactions Law*. As with the 2013 *Telecommunications Act* (see above), there are provisions that tie the revocation or suspension of ICT companies' licences to compliance with Government conditions, which has the potential to cause adverse impacts to users' rights to freedom of expression and/or their privacy. These provisions include:

- The law states that "*[w]hoever 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.*" (s38)
- Since Government-issued licenses are required for entities to become a "*certification authority*" for purposes of engaging in electronic transactions, licensees are subject to suspension or cancellation of licenses for failure to comply with Government imposed conditions. This could include requests to turn over information on the identity of users. (s28).

Computer Science Development Law (1996)

Background, Scope and Objectives

The Ministry of Science and Technology is in the process of revising the 1996 *Computer Science Development Law* which was intended to accelerate the growth of technology in Myanmar[99]. The new law is to be named the "*Information Technology Development Law*" and is being drafted with support from the Myanmar Computer Federation (MCF). A draft of the revised law has reportedly been sent to the President's Office before a public review.

[99] *Myanmar Computer Science Development Law* (1996).

Risks to Right to Freedom of Expression

Similar to the 2004 *Electronic Transactions Law*, the 1996 *Computer Science Development Law* provides for lengthy terms of imprisonment for anyone using a computer to do anything that undermines "*community peace and tranquillity*", "*national unity*" and other vague and undefined conduct (Table 18). It also puts limitations on use of ICTs. Criminal penalty could result from connecting to or establishing a "*computer network*" without MCIT permission.

Table 18: Provisions of the Computer Science Development Law with Potential to be used to Infringe Freedom of Expression

- Anyone "*using computer network or any information technology*" to engage in "*carrying out any act which undermines State Security, prevalence of law and order and community peace and tranquility, national unity, State economy or national culture*" or "*obtaining or sending and distributing any information of State secret relevant to State security, prevalence of law and order and community peace and tranquility, national unity, State economy or national culture*" may be imprisoned for 7-15 years and/or fined. (s35)
- Anyone wishing to establish "*a computer network or connecting a link inside the computer network*" must apply for prior permission from the MCIT. (s29)

Risks of Company Involvement in Human Rights Violations

ICT companies could be liable for abetting offences under the *Computer Science Development Law*. In particular:

- "*Whoever attempts or conspires to commit any offence under this law or abets in the commission of such offence shall, on conviction be punished with the same penalty prescribed in this Law for such offence.*" (s38)

This again raises the risk that if ICT companies, in order to maintain their legal licenses to operate, comply with Government measures to restrict computer use, they may as a result be involved in adverse human rights impacts caused by the Myanmar Government.

Law Relating to the Registration of Organisations (2014)

Background, Scope and Objectives

For decades the Myanmar authorities greatly restricted the right to form organisations and arrested those attempting to do so. In 1988 the military government issued a Decree called the *Associational Law* (Law No. 6/88), which named categories of banned organisations and provided for harsh terms of imprisonment and fines for people belonging to these organisations. However as part of the political, economic and legal reform process, which began in 2011, new efforts were made to change laws governing freedom of association. The culmination of such work by CSOs and Parliament was the enactment of the *Law relating to Registration of Organisations* in July 2014. The law

annulled *Law No 6/88* (Article 43), thereby increasing the political space for CSOs and others to form organisations.

Risks to Right to Freedom of Association

An early draft of the *2014 Law Relating to Registration of Organisations* required all groups to be formally registered, with severe penalties for failing to do so. The law was adopted in July 2014 with this provision removed. However it retains another provision of concern to CSOs, which requires groups who do decide to register to do so at township, state or national level. This thereby potentially restricts their area of operation, since organisations that register in one township would only be able to operate in that township.[100] The website of the International Centre for Not-for-Profit Law (ICNL) provides further information on laws relating to Myanmar civil society.[101]

Table 19: Provisions of the Law Relating to the Registration of Organisations with Potential to be used to Infringe the Right to Freedom of Association

- Prohibited organisations include those "*that attempt, instigate, incite, abet or commit acts that may in any way disrupt law and order, peace and tranquility, or safe and secure communications*" and "*Organisations that attempt, instigate, incite, abet or commit acts that may [affect] or disrupt the regularity of state machinery*" (s5)
- "*Any person found guilty of committing an offence…shall be punished with imprisonment for a term which may extend to five years*." (s6)

Risks of Company Involvement in Human Rights Violations

Read broadly, ICT companies found to be providing services to such prohibited organisations might be accused of 'abetting' them. In particular:

- Anyone found "*aiding and abetting…organisations that are not permitted to form or not permitted to continue in existence…shall be punished with imprisonment for a term which may extend to three years*." (s7)

An ICT company, to avoid liability or revocation of their license, might therefore take steps to contribute to a restriction of an organisation's right to freedom of association (or expression).

Unlawful Associations Act (1908)

Background, Scope and Objectives

A number of laws restricting freedom of expression and association in Myanmar are still in force, in spite of the legal reform process which began during 2011. Among them is the colonial era *1908 Unlawful Associations Act*.

[100] DVB, "Activists relay worries of draft association law to parliament" (5 June 2014).
[101] ICNL, "NGO Law Monitor: Myanmar (Burma)" (last accessed August 2015).

2

Risks to the Right to Freedom of Association

The *1908 Unlawful Associations Act* has often been used in the past to imprison peaceful critics of the Government. Article 15 (2) (b) defines an organisation to be unlawful "*which has been declared unlawful by the President…*" i.e. based solely on the head of state's opinion rather than on reason or evidence. Under Article 17 (1), not only can a member of an illegal organisation be imprisoned, but anyone in any way associated with an unlawful organisation is also at risk of imprisonment. Article 17 (2) provides for imprisonment of leaders of illegal organisations. Article 15 (2) (a) also defines illegal organisations as those involved in violence, often ethnic minority armed opposition groups.

While states need to protect its citizens from violence,[102] there is concern that this provision has been used against ethnic minority civilians not involved in violence. Although the *Unlawful Associations Act* is now less frequently used, ethnic minority civilians in armed conflict areas have recently been sentenced under its provisions.[103] It remains of concern to anyone involved in the peace process since non-state armed groups are considered 'unlawful associations' even though they are negotiating a nationwide ceasefire with government.

Table 20: Provisions of the Unlawful Associations Act with Potential to be used to Infringe the Right to Freedom of Association

- Under the law, "*unlawful association means an association which encourages or aids person to commit acts of violence or intimidation or of which the members habitually commit such acts, or which has been declared to be unlawful by the President.*" (s15(2))
- In addition, "*Whoever is a member of an unlawful association, or takes part in meetings of any such association, or contributes or receives or solicits any contribution for the purpose of any such association or in any way assists the operations of any such association, shall be punished with imprisonment for a term [which shall not be less than two years and more than three years and shall also be liable to fine].*" (s17)

Risks of Company Involvement in Human Rights Violations

Read broadly, an ICT utilised for the purpose of organising a meeting, or broadcasting the communications, of an "*unlawful association*" could be held liable since:

- Anyone who "*assists in the management of an unlawful association, or promotes or assists in promoting a meeting of any such association, or of any members thereof as such members, shall be punished with imprisonment for a term [which shall not be less than three years and more than five years and shall also be liable to fine].*" (s17(2))

[102] Amnesty International, "Myanmar: Justice on Trial", (July 2003), pg 28 – 33.
[103] See for example Fortify Rights, "'I thought they would kill me', Ending Wartime Torture in Northern Myanmar" (June 2014), pg 40-41 and 42-43.

Table 21: Provisions of other Domestic Laws at Risk of Infringing the Rights to Freedom of Expression and Freedom of Association and Raising Potential Liability

Freedom of Expression
Penal Code (1957) [104] **Key Provisions of Concern:** – s121: Authorises death penalty for anyone who "*incites*" the "*commission of treason*". – s123 & s124: Authorises imprisonment for anyone who "*encourages*" the commission of treason or "*by words… attempts to bring into hatred or contempt, or excites dissatisfaction (or attempts) towards*" the Government. – Although these provisions do not explicitly specify electronic communications, this could be implied from the provisions. **Provisions raising potential liability for ICTs:** – s124B: Anyone who "*knowingly or willfully prints, publishes, edits, issues, circulates, sells, distributes, or publicly displays any written or printed matter which advocates, advises, or teaches the duty, necessity, desirability or propriety of overthrowing or destroying any such organ by force or violence…shall be punished with imprisonment of either description for a term which may extend to not less than three years and not more than ten years, and shall also be liable to fine*."
Emergency Provisions Act (1950) [105] **Key Provisions of Concern:** – s5: Up to 7 years imprisonment for communication that "*alarm[s]*" people in a way that would create panic, or "*spread[ing] false news, knowing, or having reason to believe that it is not true,*" and "*affect[ing] the morality or conduct of the public/a group...in a way that would undermine the security of the Union or the restoration of law and order*". – Although this provision does not explicitly specify electronic communications, such expression could be covered by the provisions.
Official Secrets Act (1923) [106] **Key Provisions of Concern:** – s3C: Authorises imprisonment for up to 14 years for anyone who, "*for any purpose prejudicial to the safety or interests of the State… obtains, collects, records or publishes or communicates to any other person any…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*."

[104] *Myanmar Penal Code* (1957).
[105] *Myanmar Emergency Provisions Act* (1950).
[106] *Myanmar Official Secrets Act* (1923).

2

E. Guidance for Governments and ICT Companies on Meeting International Standards

Table 22: Guidance for Governments on ICT Policy and Law Making

- UN Special Rapporteur on Freedom of Opinion and Expression – Report on Freedom of Expression and Opinion on the Internet (2011)
- Representative on Freedom of the Media of the Organisation for Security and Co-operation in Europe (OSCE) – Report on Freedom of Expression on the Internet (2011)
- International Mechanisms for Promoting Freedom of Expression – Joint Declaration on Freedom of Expression and the Internet
- International Mechanisms for Promoting Freedom of Expression – Joint Declaration on Defamation of Religions, and Anti-Terrorism and Anti-Extremism Legislation
- Parliamentary Assembly of the Council of Europe – Resolution 1577
- International Principles on the Application of Human Rights to Communications Surveillance (2013)
- UN Special Rapporteur on Freedom of Opinion and Expression – Report on Surveillance of Communications (2013)
- World Summit on the Information Society – Declaration of Principles (2003)
- Internet Rights & Principles Dynamic Coalition – Internet Rights & Principles Charter

Table 23: Guidance for ICT Companies on Meeting International Standards

- Telecommunications Industry Dialogue – Guiding Principles on Freedom of Expression and Privacy (2013)
- Global Network Initiative – Implementation Guidelines (2010)
- Access – Telco Action Plan (2011)
- UN Special Rapporteur on Freedom of Opinion and Expression – Report on Freedom of Expression and Opinion on the Internet (2011)
- UN Special Rapporteur on Freedom of Opinion and Expression – Report on Surveillance of Communications (2013)

3

Chapter 3

Sector-Level Impacts

3

Chapter 3
Sector-Level Impacts

In this Chapter:

A. Introduction

As the number of Internet users, and mobile penetration rates, in Myanmar continue to increase, various opportunities and potential human rights risks require the attention of Government, private sector, and civil society organisations. This section of the Report examines aggregate or "sector-wide" impacts on human rights – both positive and negative – which can result from the ICT rollout in Myanmar. These include economic, social and governance impacts on human rights, such as the right to an adequate standard of living, education and highest attainable standard of physical and mental health.

This Chapter is intended to highlight the importance to Government of consideration of the broader implications of its policies and laws (or lack thereof). For companies, it identifies wider risks the Myanmar operating context poses to responsible business conduct and in turn the wider impacts that business operations can create for Myanmar society and therefore the wider context of its "social license to operate" beyond its legal license to operate. Where gaps exist, there may be a need for collective action, possibly with a range of stakeholders. For civil society, the Chapter sets out an overall picture of the sector and useful information on the wider impacts of the sector, both negative and positive. And finally for donors or other development partners providing support and assistance, the Chapter is a reminder of the wider context for their support, the interconnections between many of these issues and a prompt to consider the wider implications beyond the four corners of their projects.

Table 24 shows the ICT value chain that is emerging in Myanmar. Tables at the end of this Chapter provide details of some of the main companies operating in each part of the value chain in Myanmar.

Table 24: The ICT Value Chain in Myanmar with an Explanation of Key Terms

Fibre optic cable	Fibre optic cables allow for digital information to be transmitted over long distances and at high speeds. These cables are typically installed underground in trenches or underwater along ocean seabed for international Internet connectivity.
Tower companies	Tower companies are responsible for site acquisition i.e. leasing land from landowners. They often sub-contract tower construction (including civil work and tower erection). In some cases they can also manage power generation (diesel generators or hybrid with battery). Once the tower is built, they lease space on the tower to network operators who install their equipment on the tower.
Power generation	Power is required for base-transceiver stations (BTS) located at tower sites. Power is also required for larger data centres used in telecommunications. Depending on the business model, separate companies can provide and maintain diesel generators or hybrid diesel generator battery combinations for tower sites. These companies are responsible for fuel. In some cases, companies also sub-contract security to protect against tampering or fuel theft.
Network equipment providers	The role of the network vendor (or active network equipment suppliers) is typically to build, and in some cases manage, the telecommunication infrastructure that provides the basis for all fixed and mobile communications, including calls and data. A network vendor's main customers are telecoms operators (see below). A network vendor ensures that connectivity occurs across services, operators, and borders, and also ensures that the network is capable of handling the increasing demands for data and access, by supplying what is known as the "radio network". A vendor may also provide physical hardware, known as the "core network", to perform specific tasks, such as lawful interception. Once towers are constructed, the network vendor companies then fix their radio signal receiver and transmitter equipment on the tower. Transmitters can also be housed in nearby base stations, which are normally a few feet away from the tower. Mobile phones continually emit signals that are picked up by the nearest receiver on the nearest cell towers when a call is made or a text message sent. Once the call is connected, the transmitters in base stations then carry the information (such as a conversation) to the mobile phone of the intended recipient. When the user is in transit (for example on a bus) and moves out of range of one tower, the connectivity is maintained because the next closest tower picks up the communication.

Mobile network operators	Operators are companies that provide mobile and Internet services directly to the user for a fee. The telecommunications industry is generally highly regulated by governments and telecommunications operators must have on-going relationships with governments in countries where they operate, as they require licenses to operate and to obtain frequency (spectrum) allocations. The contract to provide telecommunications services is between the Government and the operator; therefore the legal obligation to provide interception capabilities (when such a law is in place) lies with the operator. Inherent in all mobile networks is the ability to find users placing or receiving a call or message in order to connect the two. Without this inherent feature, there would be no connectivity. This means that at any given time, the location of someone carrying a mobile phone must be determined. Mobile network operators routinely collect this location information mainly to use for billing purposes and to determine if a call was made locally, or while roaming nationally or abroad.
Internet service providers	Internet service providers (ISPs) provide customers with access to the global Internet, usually for a monthly or hourly fee. Internet service providers can offer fixed line or wireless connections. Mobile network operators also typically function as Internet service providers, as customers pay for wireless data access.
Web based service providers	Web based service providers, (sometimes referred to as 'Over the Top' service providers) provide online services or platforms for users. This includes social networking, search engines, e-commerce, messaging applications, or cloud computing services.
Software developers	Software developers create applications that run on ICT hardware, including mobile phones, wearable technology (e.g., smart-watches), laptops, desktop computers, and servers.

B. The Current State of the ICT Sector in Myanmar

The Current State of Telecommunications

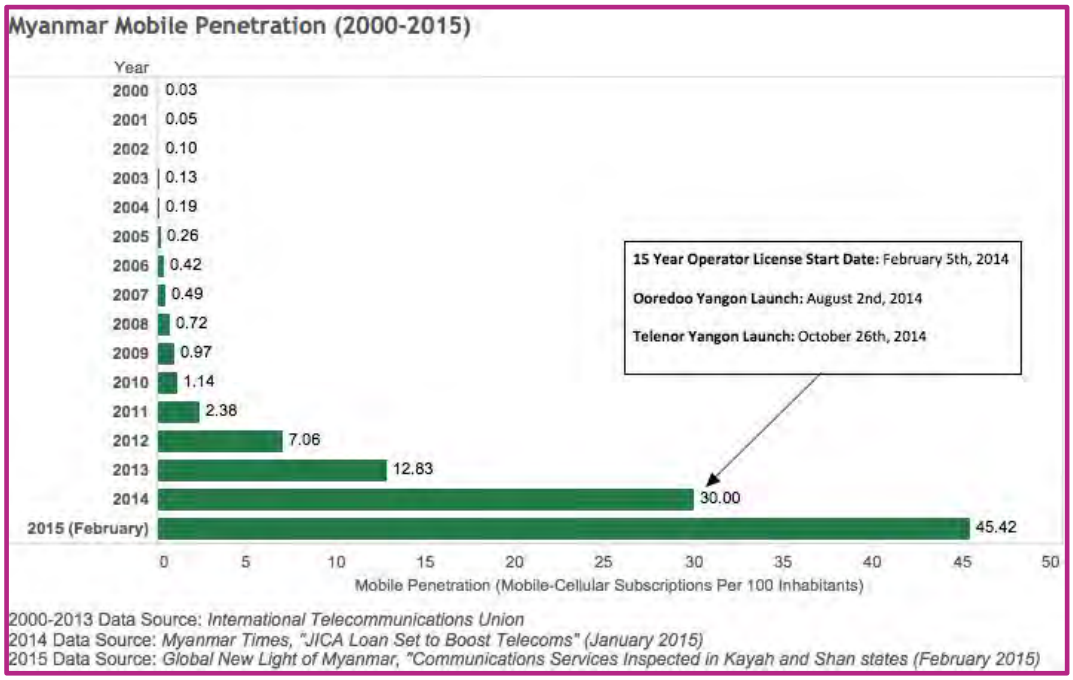
Until 2012, Myanmar was at the bottom of the global league table for mobile penetration. In 2012, only North Korea (6.97%) and Eritrea (4.98%) had lower mobile penetration rates than Myanmar (7.06%)[107]. However, mobile penetration rate has increased rapidly since

[107] International Telecommunications Union, "Statistics: Time Series by Country, Mobile Cellular Subscriptions" (last accessed August 2015).

then. The 2014 Census reports that 32.9% of the population had access to a mobile phone at the time the census was conducted in March-April 2014.[108] In the first quarter of 2015, Myanmar added more mobile subscriptions than any country in the world except for India and China.[109] A recent study of ICT needs and usage across 8,400 households in Myanmar found, amongst other things, that more than 90% of the wards/villages have coverage (i.e. can get a signal) and have re-load locations for topping up mobile pre-pay credit. However the purchase of SIM and handset was still limited to urban areas.[110]

The Ministry of Communication and Information Technology's (MCIT) policy framework for developing Myanmar's telecommunications sector centres on increasing overall tele-density/mobile penetration, improving the affordability of telecommunication services in urban and rural areas, and providing the population and enterprises the freedom to choose their telecommunications services and providers.

Figure 2: Myanmar Mobile Penetration Rate 2000-2015



National Telecommunications Rollout

Issuing telecoms operator licenses provided an opportunity for the Government to set ambitious targets for improvement in the coverage and types of ICTs on offer in the country. MCIT awarded 15-year operator licenses to wholly owned subsidiaries of Norway's Telenor Group (Telenor Myanmar Limited), and Qatar's Ooredoo (Ooredoo Myanmar Limited) that took effect on 5 February 2014.

[108] The Republic of the Union of Myanmar, "2014 Myanmar Population and Housing Census, Census Report Volume 2-A" (May 2015).
[109] Myanmar Times, "Myanmar third for mobile grown" (15 July 2015).
[110] See further, H Galpaya, "Knowledge, information and communication habits and needs in Myanmar: Stories from the field" ICTD2015 Conference (May 2015).

The targets included in the licences set out an ambitious vision for improvement of voice and data service coverage throughout the country:

- "Commercial launch no later than 9 months after the effective date of the Licence;
- Geographic coverage for voice services of 25% and for data services of 10% within 12 months;
- Geographic coverage for voice services of 75% and for data services of 50% within 60 months."[111]

The two international licensees each achieved 1 million subscribers within the first 2-3 weeks of operations.[112]

Each operator licence includes the requirement that after three years (assuming network rollout targets are met) each operator must contribute 2% of annual revenue to a Universal Service Fund managed by MCIT. This Fund is intended to subsidise the cost of telecommunications service in areas where infrastructure deployment is not economically viable for network operators. (For more on universal service, see below under "Cost of Telecommunications Access").

To support the rollout targets, MCIT also issued new draft rules for the telecommunications sector relating to Licensing, Access and Interconnection, Spectrum, Numbering and Competition, which was open for public consultation in November 2013.[113] Each class of licence permits companies to engage in the specific activities set out in Table 25 below. As of April 2015, MCIT issued several types of licences to 20 companies to provide these telecommunications services. These licences differ from the licences to operate national telecommunications networks held by Telenor, MPT, and Ooredoo. See also Tables 33 and 34 at the end of this chapter for further information.

Table 25: Classes of Telecommunications Licences in Myanmar

Class of Telecommunications Licence	Example of activities
Network Facilities Service (Individual)	Construct, maintain, operate, and provide telecommunications services over: ■ Terrestrial fixed line transmission facilities ■ Terrestrial radio transmission facilities ■ Mobile base stations ■ Submarine cable facilities

[111] New Light of Myanmar, "Telecommunications Operator Tender Evaluation and Selection Committee issues press release" (28 June 2013), pg 5 and 16.
[112] TowerXchange, "The Myanmar tower rollout: FAQs (updated June 2015)".
[113] See the draft rules here http://www.mcit.gov.mm/content/proposed-rules-telecommunications-sector.html and comments by MCRB http://www.myanmar-responsiblebusiness.org/news/comments-mcit-proposed-rules-telecommunications-sector.html

	■ International Gateway Services facilities ■ Satellite earth station facilities ■ Other Myanmar-based satellite facilities that can transmit telecommunications services
Network Facilities Services (Class)	Deploy and maintain passive network infrastructure for civil engineering and non-electronic elements, including but not limited to: Towers; Masts; Ducts; Trenches; Poles; Dark fibre.
Network Services	Provision of the following telecommunications services: ■ Resale of wire-line connectivity services ■ International and domestic network transport and switching services ■ Resale of International Gateway Services
Application Services	Provision of the following telecommunications services: ■ Public payphone services ■ Public Switched data services ■ Audio text hosting services provided on an opt-in basis ■ Directory services ■ ISP services ■ Public Access centre services ■ Messaging services ■ Private line voice and/or data services (including leasing Wide Area Network capacity to third parties) ■ Value-Added services

Source: VDB-LOI, "Telecom Myanmar Update" (September 2014)

Improving Coverage and Mobile Phone Reception

Mobile towers provide improved reception for mobile phone users. Each mobile tower has a range of 1-5 miles; the closer the user is to the tower the better their signal will be. Nearly eight months after the launch of Telenor and Ooredoo, mobile towers dot the rural horizon or are perched on rooftops in many of Myanmar's major cities. As of March 2015 there were over 5,000 mobile towers providing voice and data coverage to Ooredoo, Telenor, MPT, and MECtel customers (see further the Tables at the end of this chapter).

On average a mobile tower can take approximately 3 weeks to construct, excluding weather delays, or difficulties obtaining the required permits authorising land use, re-zoning, and construction. Each operator has subcontracted land acquisition and construction to specific tower companies, who typically subcontract elements of the process (e.g. civil work) to additional companies. By May 2015 it was reported that the two international mobile network operators had signed a second round of purchase orders

for telecommunications towers after long delays due to protracted negotiations over pricing and terms.[114]

MCIT has not succeeded in implementing infrastructure sharing (i.e. requiring that towers host the network equipment of more than one operator). This means that each operator and their contractors are continuing to aggressively hunt and compete for tower sites in order to achieve their necessary area coverage to meet rollout targets. Slowing down the site leasing process to adequately engage communities during the scoping and construction phase of locating towers to hear and address their concerns works against this market and contractual imperative. This reflects a broader challenge operators currently face in Myanmar, between aggressive rollout commitments on the one hand and the need to ensure responsible and effective business practices that requires sufficient time and resources to implement. This is an example of a gap in Government approach that creates a disincentive for responsible business conduct.

Cost of Telecommunications Access

Prior to the licencing of new mobile network operators in Myanmar, SIM card prices had historically been high, often costing thousands of US dollars. In April 2013, the State-owned Myanma Posts and Telecommunications (MPT) began selling SIM cards to winners of a public lottery at a price of 1,500 MMK (around $1.50).[115] During the lottery's first month, an initial batch of 320,000 SIM Cards was made available with each administrative ward receiving a limited allocation of 100 SIM cards.[116] Many lottery winners sold their SIM cards to third party brokers and phone shops. Overall SIM prices were reduced, but black market prices remained too high for most users to afford.

Telenor and Ooredoo also began selling SIM cards for 1,500 MMK in the latter half of 2014 when their networks were launched. Android smartphones can now be purchased for as little as 50,000 MMK, in some areas, making owning a mobile phone with Internet access financially realistic for many people for the first time in Myanmar's history. In May 2015, the Union Parliament suspended a newly imposed 5% commercial tax on mobile phone top-ups until the next fiscal year following public dissent.[117] Similarly, in July 2015, state-owned Myanma Posts and Telecommunications (MPT) halved the price of landline phone installation. The rate had previously been 650,000 MMK (roughly $565) – well beyond reach for the majority of households, and was brought down to 325,000 MMK, potentially signalling a Government priority to liberalise the fixed line market.[118]

In August 2015, MCIT launched a tender for the design of Myanmar's universal service strategy. The tender outlined support for MCIT and the regulator Post & Telecommunications Department (PTD), and the universal service strategy's implementation in a number of pilot areas, in order to "accelerate the development of rural

[114] Myanmar Times, "Bad reception Telenor and Ooredoo pick new tower firms" (25 May 2015).
115 Reuters, "In Myanmar, cheap SIM card draw may herald telecoms revolution" (24 April 2013)
[116] Telegeography Research Services, "Govt: You Can't Win the SIM Card Lottery if You Don't Buy a Ticket" (April 2013)
[117] Myanmar Times, "Parliament suspends 5% tax on top-up" (28 May 2015).
[118] Irrawaddy, "State-Owned Telecom Slashes Landline Fees as Users Go Mobile" (15 July 2015).

telecommunications infrastructure and services in locations that are unlikely to attract sufficient private investment."[119]

The Current State of Internet Infrastructure and Internet Services

The nation-wide rollout of telecommunications networks in Myanmar comes at a time when the reach of the global Internet has reached an unprecedented scale. Globally, there are now more Internet-connected devices than people.[120] Many users in Myanmar are connecting to the Internet for the first time. While mobile penetration has steadily increased following the Ministry's liberalisation of the sector, fixed-line Internet penetration remains low. The 2014 Census reports that as of March-April 2014 only 6.2% of the population had access to the Internet at home.[121] ISPs have struggled to balance Myanmar's limited Internet capacity with customer demand. In November 2014, MPT and Yatanarpon Teleport stopped accepting applications for new fibre connections, in order to concentrate on increasing capacity of existing connections.[122]

Internet Rollout

While new mobile towers have improved voice coverage nationally, Internet speed remains poor due to the quality of Myanmar's underlying Internet backbone and an immense demand for Internet services. Connectivity to the global Internet is important, because the majority of content users are attempting to access is hosted on servers outside Myanmar. This includes Myanmar specific content and international software services. For example, the popular Myanmar language news site "7 Day News" is currently hosted on servers maintained by Amazon Web Services in Singapore.[123] For many Myanmar companies, the decision to host their website outside Myanmar is due to lower cost and increased reliability of electricity. Popular services such as Facebook, Google Search and Gmail, YouTube, and Viber also require international Internet access. These services connect with servers located outside of Myanmar, where data is stored and processed. For example, Google currently has 13 data centres globally, all located outside of Myanmar.

As far back as the 1990s, the workings of the Internet backbone were compared to a road freeway or highway system by experts and politicians.[124] One component of a strong backbone is the collection of fibre optic cables that can be either submarine or terrestrial. The way information travels along these cables and is routed to different places is similar to vehicles travelling along lanes on a highway. Not only does Myanmar currently have a limited number of lanes for information to travel around the country, Myanmar also has a limited number of lanes connecting users to the global Internet. Myanmar is currently served by only one submarine Internet cable, South East Asia-Middle East-Western-Europe-3. Myanma Posts and Telecommunications (MPT) is a member of global

[119] See MCIT, "Invitation for Expression of Interest: Myanmar's Universal Service Strategy" (6 Aug. 2015).
[120] See: https://www.apnic.net/
[121] The Republic of the Union of Myanmar, "the 2014 Myanmar Population and Housing Census, Census Report Volume 2-A" (May 2015).
[122] Aung Kyaw Nyunt, "Fiber Connection Freeze from Leading ISPs", Myanmar Times (November 2014).
[123] See Website and IP location at http://check-host.net/ip-info?host=http://www.7daydaily.com/.
[124] See US Vice President Al Gore's "Speech at Royce Hall, UCLA Los Angeles, California" (11 January 1994). See also Page 6, Nicholas Economides, "The Economics of the Internet Backbone" (2005).

consortium for the South East Asia–Middle East-Western Europe 5 cable and the Asia-Africa-Europe-1 cable and will also jointly manage the AAE-1 cable landing station in Ngwe Saung in 2016.[125] The addition of these international links, combined with further over-land fibre optic cables extending into neighbouring countries Thailand, India, and China will improve the capacity of Myanmar's Internet. Private companies such as Singapore's Campana Group have announced plans to deploy additional submarine cable.[126] Other firms are installing thousands of kilometres of terrestrial fibre cable inside Myanmar, providing increased connectivity to major cities and last mile connectivity to remote areas.

Currently, if many Internet users are streaming videos, downloading music, and posting photos at the same time, there will be a 'traffic jam' as bandwidth is congested. As of January 2013, Myanmar Computer Federation estimated Myanmar's Internet backbone bandwidth to be 14 gigabits per second.

Table 26: Comparison of Broadband and Mobile Download Speed across ASEAN

Country	Average Broadband Download Speed	Average Mobile Download Speed
Singapore	121.8 mbps	17.5 mbps
Thailand	19.9 mbps	5.4 mbps
Vietnam	18.5 mbps	1.7 mbps
Cambodia	9.1 mbps	5.8 mbps
Brunei	7.7 mbps	10.1 mbps
Malaysia	7.0 mbps	6.6 mbps
Indonesia	6.5 mbps	4.1 mbps
Myanmar	6.5 mbps	2.5 mbps
Laos	5.8 mbps	3.1 mbps
Philippines	3.6 mbps	4.4 mbps
ASEAN Average	20.64 mbps	6.12 mbps

Source: Net Index, May 5th, 2015

Table 27: Case Study from the ASEAN Region – Vietnam

Part of Vietnam's development strategy is to strengthen the information and technology sector by spreading countrywide broadband information infrastructure, through wireless broadband.[127] From 6.9 million subscribers of mobile data communications in 2008, the figure was estimated to rise to 22.4 million in 2014. The number of mobile subscribers will reach 23 million, giving the country tele-

[125] Submarine Cable Networks, "China Unicom Announces to Land AAE-1 Cable in Myanmar" (November 2014) and "SEA-ME-WE 5 Consortium Concludes Construction Agreement" (March 2014).
[126] Myanmar Times, "MYTHIC set to compete" (February 2015).
[127] International Telecommunications Union "Wireless Broadband Masterplan for the Socialist Republic of Viet Nam" (October 2012).

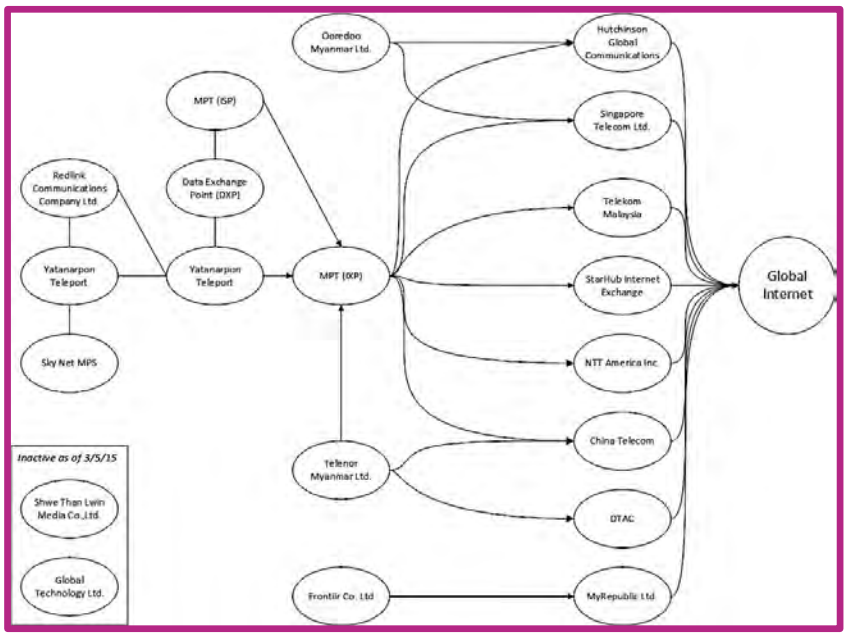
density (number of mobile phones for 100 people) of nearly 141 percent, among the highest such figures in the world (up from 130 in 2011).[128] The growth is fuelled by the increased use of pre-paid technology and easier availability of low-cost handsets.

The International Telecommunication Union's ICT Development Index (IDI) which measures countries across the digital divide and potential showed in its 2011 report[129] that Vietnam had increased its IDI score from 2.76 in 2008 to 3.53 in 2010, ranking 81st out of 152 nations measured. The growth was primarily due to increased broadband penetration.[130]

Current Configuration of Access to Global Internet

The diagram below is a simplified version of how Myanmar's Internet traffic is routed to the global Internet through high-speed hubs.

Figure 3: How Myanmar's Internet Traffic is Routed



Source: Yatanarpon Teleport, Hurricane Electric BGP Tool Kit, http://bgp.he.net/ (May 2015)

While the diagram demonstrates an increased number of companies offering international Internet connectivity, it also shows that Myanmar is still at risk of an Internet service disruption due to the current configuration of Internet services[131]. MPT carries the majority of Internet traffic, including serving approximately 8.4 million mobile customers (Telenor

[128] According to some reports, Vietnam's tele-density now stands at 145 per 100 people. (See: https://www.techinasia.com/vietnam-100-people-145-mobile-phones)
[129] ITU, "Measuring the Information Society" (2011).
[130] Tuoitrenews, "One in three Vietnamese use smartphones" (13 September 2014).

[131] 'Fibre cuts slow internet speeds', Myanmar Times, 17 August 2015

and Ooredoo currently serve 6.4 million and 3.3 million mobile customers respectively).[132] If MPT's routing were disabled, this would effectively disable Internet access for 8.4 million mobile subscribers, and fixed-line Internet subscribers from Redlink (wireless broadband), Elite fibre to the home, Fortune fibre to the home, and Yatanarpon Teleport from accessing the global Internet.

Cost of Internet Access

The price of Internet access in Myanmar (both fixed line and mobile) remains a barrier for many potential customers. A study of broadband infrastructure in the ASEAN region by the United Nations Economic and Social Commission for Asia and the Pacific (UNESCAP) highlighted the disproportionate cost of Internet access in Myanmar relative to nominal GDP per capita compared to its ASEAN neighbours.

Table 28: Comparison of Broadband Access Costs Across ASEAN

Country	1Mbps broadband subscription (including installation) as a percentage of nominal GDP per capita
Myanmar	132.8%
Cambodia	48.75
Lao PDR	27.4%
Philippines	11.2%
Vietnam	7.05%
Indonesia	5.5%
Thailand	0.5%
Singapore	0.1%

Source: UNESCAP, "An In-Depth Study of Broadband Infrastructure in the ASEAN Region" (August 2013)

In March 2015 Myanmar joined the Alliance for Affordable Internet (AFAI). The Alliance is an ICT sector coalition that focuses on combining advocacy, research, and knowledge sharing to influence broadband policy. AFAI's goal is to realise the "UN Broadband Commission's target of entry-level broadband priced at less than 5% of monthly income".[133] Following a signing ceremony in Yangon, a multi-stakeholder meeting was held between members of civil society, private sector and Government[134] to establish priority areas for implementation in Myanmar which were identified as infrastructure sharing, taxation, data collection, and a Universal Service Fund. Quarterly multi-stakeholder meetings are envisaged. While it is unclear how all this will be implemented, Myanmar's draft Telecommunications Masterplan has outlined some first steps, including the aspiration that broadband Internet expenditure for typical usage does not exceed 5% of Myanmar citizens' income.[135] The approach of working through sector issues in a multi-

[132] Jared Ferrie, "SIM Sales Soar as Myanmar Races to Catch Up in Telecoms" (May 2015)
[133] Alliance for Affordable Internet, "Vision and Strategy" (last accessed August 2015).
[134] Alliance for Affordable Internet, "Working Toward Universal, Open & Affordable Internet in Myanmar" (March 2015).
[135] See Myanmar "Draft Telecommunications Masterplan" (July 2015), pg. 7.

stakeholder way is something that would have been unprecedented even a few years ago.

C. Sector-Wide Impacts

Economic Impacts

In the 2014-2015 fiscal year, foreign investment in the telecommunications sector in Myanmar has been estimated to contribute over $2 billion of $8.1 billion in total foreign direct investment (FDI).[136] In terms of total FDI, the Myanmar Directorate of Investment and Company Administration (DICA) ranks 'Transport and Communication' fourth behind oil and gas, power, and manufacturing.[137]

A robust ICT sector can be economically transformative, reshaping existing industries through increased efficiency and productivity, facilitating cross-sector growth, and raising GDP per capita. The World Bank has estimated that in developing countries, a 10% increase in tele-density (defined as the number of telephone connections per 100 people) correlates with a 0.8% increase in GDP per capita, while a 10% increase in Internet penetration (Internet connections per 100 people) and broadband penetration (broadband connections[138] per 100 people) result in 1.12% and 1.38% increases in GDP per capita respectively.[139]

It has been estimated that by 2030 the ICT sector could contribute $6.4 billion to Myanmar's GDP and employ approximately 240,000 people.[140] It will be important however, for the Government and companies investing to consider what is appropriate technology for the country. Some types of ICT are more appropriate to the Myanmar context now and in the near future and therefore represent higher priorities, while other technologies may represent high costs, with low benefits, given its state of development.

Impacts on Agricultural Productivity

ICTs can improve the availability and sharing of market information (pricing and demand), via SMS text messaging or voice calls. The agricultural value-chain in Myanmar is comprised of farmers, fisherman, input suppliers (seeds, fertiliser, pesticide, etc.), processors, brokers, direct buyers, and transport/logistics providers. While specific studies on the economic impacts of ICTs on Myanmar's agricultural sector are lacking, the World Bank notes that in other regional markets the effect of increased market information from ICTs on farmer income and prices is generally positive, while traders leveraging ICTs can

[136] Deal Street Asia, "Myanmar 2014-15 FDI Swells to 8.1b: Govt Agency" (April 2015).
[137] See DICA's "Foreign Investment by Sector (April)" (last accessed August 2015).
[138] The World Bank defines broadband as high-speed access to the public Internet (a TCP/IP connection), at downstream speeds equal to, or greater than, 256 kbit/s. This includes cable modem, DSL, fiber-to-the-home/building and other fixed (wired)-broadband subscriptions.
[139] Christine Zhen-Wei Qiang, "Mobile Telephony: A Transformational Tool for Growth and Development", (4 May 2015).
[140] McKinsey Global Institute, "Myanmar's Moment: Unique Opportunities, Major Challenges" (Jun 2013),p43.

also boost margins.[141] Outside of providing market information, ICTs can also be used to distribute pest or weather alerts and subsequent management advice. In Myanmar, Ooredoo has released a mobile agriculture application called 'The Farmer' which is designed to promote knowledge sharing among farmers, and to boost crop yields through highlighting best agricultural practices.[142] In the future, technologies like wireless sensing will improve farmer's ability to collect and utilise information. This might include measuring the nutrient content of soil or measuring nitrogen levels in crop, which can further boost productivity.[143]

Impacts on Small and Medium Sized Enterprises (SMEs) and Services

Increased access to market information through ICTs is also impacting SMEs. During MCRB's field research, merchants in Shan State noted that ICT usage has decreased travel time and logistics cost. Instead of traveling to the Chinese border at Muse to assess market conditions, merchants now use messaging applications such as Line, WeChat, and Viber to check available stock, coordinate bulk purchases, and arrange transport for goods e.g. textiles from Muse to Taunggyi.

Adoption of ICTs is supporting the growth of new businesses and start-ups in Myanmar. Improved telecommunications access has also resulted in new payment options for e-commerce. Myanmar's national payment network recently offered cardholders (nearly 900,000 in Myanmar) the ability to pay for purchases online using their debit cards.[144] While logistics and shipping pose a challenge to e-commerce providers in Myanmar, local e-commerce offerings are beginning to emerge.[145] McKinsey estimates that Myanmar's consuming class could expand to 19 million people by 2030.[146] Services are also experiencing growth. A call centre based in Yangon serving customers of mobile-network operators reports receiving around 30,000 calls per week.[147]

In addition to e-commerce platforms and services, start-ups have emerged in Myanmar offering educational mobile applications, classified listings for automobiles and jobs, health services, social networks, and search-engines. Many start-ups continue to face operational challenges including hiring qualified employees and accessing capital. To support entrepreneurship, UNESCAP has recommended that policy makers "*subsidise start-up costs partially through seed capital and start-up loan programmes*".[148] While access to capital is a problem, ICT start-ups face additional challenges related to 'copy-cat' applications given Myanmar's lack of intellectual property protections and challenges monetising their services. Paid applications or direct carrier billing are currently not available in the Google Play app store, forcing start-ups to rely on advertising revenue.

---

[141] The World Bank aggregated data from 10 regional studies measuring the impacts of additional market data facilitated by ICTs on farmers, traders, and consumers. See Page 208 of the World Bank's "ICT in Agriculture Sourcebook" (last accessed August 2015) for further analysis.
[142] For further information, see Ooredoo Myanmar "mAgriculture" (last accessed August 2015).
[143] The World Bank, "Increasing Crop, Livestock, and Fishery Productivity through ICT" (2012).
[144] "2C2P and Myanmar Payment Union Launch Myanmar's First E-Commerce Payment Platform"(Feb 2015)
[145] See http://www.kaymu.com.mm/ and http://www.zawgyimart.com/
[146] McKinsey Global Institute, "Myanmar's Moment: Unique Opportunities, Major Challenges" (Jun 2013) p59.
[147] Mizzima, "I didn't expect the market to open so fast" (February 2015).
[148] UNESCAP, "A New Policy Framework for Myanmar's SME" (February 2014), p26.

Impacts on Tourism

ICTs are supporting the growth of the tourism sector in Myanmar, which was estimated to contribute $905 million to the Myanmar economy in 2014.[149] In September 2014, the Ministry of Immigration and Population launched an e-visa system, available to tourists from 41 countries.[150] This system is accessible online, allowing tourists to apply for and pay the visa fee online. Tourist visa are usually approved in 72 hours. ICTs are also supporting improvements to booking and reservation management for airlines and hotels. Most of Myanmar's major airlines now offer online ticketing options, while hotels and guesthouses are listing rooms on websites such as Agoda, Expedia or Booking.com (to the detriment of local hotel and flight booking agents)[151]. In top tourist destinations such as Bagan and Inle Lake, small business owners are using social media to promote their services to visiting tourists and build a brand. Tourists are able to post reviews and photos, which can increase (or decrease) repeat or future business.

Improved telecommunications is also supporting expanded payment options for visitors. While still not widely accepted, some restaurants and hotels are beginning to accept payment by credit card. This, in addition to the number of ATMs now in operation throughout Myanmar's major cities, provides tourists with greater flexibility to make unplanned purchases for example of souvenirs and crafts, providing local economic benefits.

Impacts on Migration – Communication and Remittances

MCRB's field assessment found that it remains common for recent graduates of technological universities in Myanmar to migrate to Thailand or Singapore for better job opportunities. While a new graduate could earn $200-$300 per month at a local Myanmar ICT company, field research indicated entry-level salaries in comparable roles ranged from $1300 to $2000 per month in Singapore.

Remittances from skilled and unskilled Myanmar migrant workers provide essential support to livelihoods, education, and health.[152] It is estimated that inbound remittances to Myanmar total approximately $8 billion per year with half of transactions taking place outside of formal systems.[153] This is approximately 13% of Myanmar's $59.4 billion 2012 GDP.[154] While some are able to send money home with friends, many rely on informal systems such as the 'hundie' network for remittances. This system is based on a network of agents and brokers who can transfer money between countries. Fees can range from 0.01 to 2% depending on exchange rate fluctuations. In other informal transfer systems fees can reach as high as 20%.[155]

---

[149] Mizzima News, "Myanmar Tourism to Earn US$900 Million in 2014, (December 2014).
[150] The Straights Times, "Myanmar Targets 5 Million Tourists with E-Visa" (September 2014).
[151] Myanmar Times "Local tourism companies face online competition" (26 May 2015).
[152] Andy Hall, "Myanmar Migrant Workers, Briefing and Recommendations" (April 2012).
[153] Aye Thidar Kyaw, "Hundi Remittance Lives On" Myanmar Times (July 2014).
[154] UNDATA, "Myanmar 2012 GDP Data" (last accessed August 2015)
[155] Gwen Robinson, "The True Cost of Expat Workers Sending Cash Home Remain Hidden" Financial Times (March 2013).

Informal systems are generally based on trust and personal relationships, leaving customers with few options for remedy if complications arise during the remittance process. Use of ICTs (both online banking and mobile money) provides an opportunity for increased transparency and accountability for both parties involved in the transaction. Use of ICTs can also improve the speed, reliability, and convenience of sending money domestically and internationally.

Furthermore, the enhanced connectivity of the country now means that Myanmar banks can offer online banking services and international remittances or payments. There are currently four banks[156] permitted by the Central Bank of Myanmar to provide formal remittance transfer from Malaysia, Singapore, and Thailand through partner banks. Fees for remittance services may be flat rate or variable rate, depending on the bank's partner agreements and the total amount of money being sent.

However, usage of formal money transfer systems is limited for a variety of reasons. For some, proximity to bank or money transfer branches is problematic. In many rural communities, bank or transfer branches do not exist. In the event that branches are nearby, many are reluctant to use formal services due to a broader distrust of Myanmar's banking system. Required paperwork is also problematic for migrants, some of whom do not have national registration cards, work permits, or passports. Alternative money transfer services such as Western Union, Money Gram, and Xpress Money are also now available in Myanmar due in part to increased connectivity, but often include higher transaction fees than using the hundie system.

Mobile Banking and Mobile Money

Distrust of the formal banking system is rooted in historic experiences such as demonetisations of Myanmar's currency in the 1980s and the 2003 bank runs. MDRI-CESD has estimated that formal banking penetration is only around 10% in urban areas and "*considerably lower in rural areas*".[157] Sending money in Myanmar can be time-intensive and unreliable for both banked and unbanked individuals. If an individual does not use a bank account, transferring in money may require someone to hand carry or ship the money on a bus to its intended destination. 'Carrying costs' are often deducted along the way by couriers, resulting in short payments or receipt disputes.

As mobile penetration continues to increase in the country, there is an opportunity for a variety of new financial services that utilise mobile technology. Online banking (sometimes differentiated as 'mobile' or 'Internet' banking) typically refers to customers accessing formal banking services through a mobile or desktop device connected to the Internet. For mobiles, a bank-specific smartphone application is typical, whereas desktop access is typically through a bank's website. In Myanmar, a variety of banks currently offer online banking services which allow customers to view their account balances, send money to fellow customers, check exchange rates, and find ATM locations nearby. In order to use

[156] Asia Green Development (AGD), AYA, KBZ and CB Banks
[157] See, MDRI-CESD, "Cash In Context: Uncovering Financial Services in Myanmar" (2015), pg 15.

an online banking service (app or desktop based), a user would need to be a bank customer with a checking or savings account.

In contrast to online banking, mobile money (or mobile payments) services are targeted towards unbanked users. Two thirds of Myanmar's population live in rural areas. A recent report on financial inclusion by Proximity Designs noted long physical distances from a village to the bank and limited business hours deter potential customers who already perceive setting up a formal bank account as a complicated, time intensive process.[158] Mobile money services attempt to address these issues through a simplified new customer registration process and a network of agents located throughout the country providing cash in and cash out services. After adding money to their account, a user is able to send money to other users, or pay for goods such as mobile top up. For money transfers, mobile money can increase convenience as well as enhance transparency, eliminating transport costs and creating a digital record of transactions visible on both sides of the transaction.

In December 2013, the Central Bank of Myanmar issued the "*Mobile Banking Directive*" allowing banks to offer mobile money services.[159] The Central Bank of Myanmar is reportedly in the process of drafting mobile money regulations that would allow entities outside of financial institutions – such as mobile network operators – the ability to provide mobile money services. Telenor has announced plans to partner with Yoma Bank to offer mobile money services, pending the necessary regulatory frameworks for non-bank-led mobile payments.[160] While Ooredoo has not announced specific mobile money plans for Myanmar, Ooredoo is a member of the GSMA's Mobile Money Interoperability (MMI) Programme. MPT and MECtel have partnered with Myanmar Mobile Money. In addition to targeting domestic payments, some operators have expressed interest in also targeting international remittances from sent from Myanmar to migrant workers in Thailand and Malaysia.[161]

Governance impacts

This section examines the ICT sector's contribution to improved governance in Myanmar through its ability to enable inclusive engagement between citizens and Government, increased transparency, accessibility of information, and citizen participation. Positive governance impacts can occur through e-Government programs, commitment to open governance, and civic technology (see Table 29).

[158] See Proximity Designs, "Afford Two, Eat One: Financial Inclusion in Rural Myanmar" (2014), pg 83.
[159] Edwin Vanderbruggen and Altas Dharamsi, "Easy Money? Mobile Banking, Mobile Money, and Myanmar's Financial Regulation" (May 2014).
[160] Jeremy Mullins, "Stay Tuned for Mobile Banking Services from Yoma and Telenor say CEOs", Myanmar Times (November 2014).
[161] On 21st May 2015, Telenor Myanmar held Sustainability briefing in Yangon. During the Q&A portion of this session, an audience member asked about Telenor's mobile money plans. Telenor Myanmar explained that pending needed regulation, Telenor Myanmar would partner with Yoma Bank. Longer term, Telenor Myanmar indicated they are hoping to partner with Telenor Thailand (DTAC) or Telenor Thailand (DiGi) to pursue international remittances through mobile money.

3

Improving Open Governance & the Open Government Partnership (OGP)

The Myanmar Government has committed to joining the Open Government Partnership (OGP) by 2016. The OGP is an international platform of 68 governments aimed at making their governments more open, accountable, and responsive to citizens. However Myanmar is not yet eligible to participate in the OGP. Prospective members are evaluated on objective data using a point system and must earn a minimum score of 75 across four categories: fiscal transparency, asset disclosure by public officials, access to information, and citizen engagement. In addition, prospective members must make a specific commitment to the OGP principles and develop an effective consultation process with civil society to develop a national action plan.[162]

OGP is about changing the culture of government to one where it is open by default and where citizen participation is a routine part of policy development. If citizens can engage in public debate, provide input, and make contributions this will lead to more responsive, innovative and effective governance. OGP is particularly about promoting accountability, requiring government actors to justify their actions, act upon criticisms or requirements made of them, and accept responsibility for failure to perform with respect to laws or commitments. If the Government of Myanmar carries through with its commitments to the OGP, the initiative has the power to transform the relationship between the Government and its citizens through the use of ICT.

Although the Government Steering Committee and Working Committee have been announced, both committees lack a website or readily available public information on their plans and activities, and also lack diverse stakeholder representation, including civil society participants. Myanmar CSOs have raised concerns that there may be more pressing priorities than OGP including constitutional reform, justice and a genuine peace process, rule of law, and urgent legal and judicial reform.[163]

Table 29: The Emergence of Civic Tech[164]

Focus Area	Definition
Visualisation and Mapping	Enable users to make sense of and gain actionable insight from civic data sources, specifically through the visualisation and mapping of that information
Data Utility	Empower users to analyse Government data and leverage data to improve service delivery
Data Access and Transparency	Promote Government data availability transparency and accountability
Voting	Support voter participation and fair election processes
Public Decision Making	Encourage resident participation in large-scale deliberative democracy and community planning efforts
Resident Feedback	Provide residents with opportunities to interact with Government

[162] See OGP, "How to Join" (last accessed August 2015).
[163] Burma Partnership, "Statement from Open Government Partnership Awareness Workshop for Civil Society" (January 2015).
[164] See: Knight Foundation, "What does the civictech landscape look like?" (last accessed August 2015).

	officials and give feedback about public service delivery

Source: Knight Foundation, "The Emergence of Civic Tech: Investments in a Growing Field" (2013)

E-Governance Master Plan

See Chapter 2 on ICT Government Institutions, Policies and Legal Framework.

ICTs and Law Enforcement

During the 2007 Saffron Revolution, ICTs facilitated the flow of information domestically and internationally, highlighting the violent Government crackdown on peacefully protesting Buddhist monks, even though mobile penetration in Myanmar was less than 1%. Today, national mobile penetration is approaching 50%. As more people in Myanmar have access to mobile devices with cameras, this has increased transparency around the conduct of law enforcement. In March 2015, photos and video of student protesters in Letpadan being beaten by police were uploaded online and ICT users accessed local and international news reporting on the protests from their mobile devices.

ICTs can support checks and balances on law enforcement. But law enforcement is also expanding operations into the digital realm. Following police crackdown on student protesters in Yangon, activists reported their phones being tapped and social media accounts being hacked by law enforcement agencies. (See 4.4 Surveillance)

Table 30: Case Study on ICTs and the Kenya Election

The disputed 2007 Presidential election in Kenya resulted in an outbreak of post-election violence that left over 1,000 people dead and over 600,000 people displaced. Post-election inquiries into the violence acknowledged the role of SMS messages and online blogs in exploiting tensions between ethnic communities and inciting violence.

In the run up to the 2013 elections, concerns of another outbreak of violence and fears over the potential of SMS to simultaneously send messages that incite violence led the Kenyan mobile operator Safaricom to take action. Recognising the potentially negative role of bulk SMSs sent by politicians during the last elections, Safaricom decided to develop its own code of conduct in vetting bulk SMS content that political parties, politicians and aspirants wished to send in the run up to the 2013 elections. In 2012, Safaricom developed *Guidelines for Political Mobile Advertising on Safaricom's Premium Rate Messaging Service.*[165] Under these guidelines, anyone intending to send bulk SMS of a political nature would first have to submit an application to Safaricom, which would vet the content to ensure they did not contain instances of hate speech. In addition to this, Safaricom sought and received the support of the Government and the Communications Commission of Kenya (CCK) to develop and

[165] Bloggers Association of Kenya, "Safaricom Issues Tough Guidelines For Political Messaging" (15 June 2012).

release *Guidelines for the Prevention of Transmission of Undesirable Bulk Content/Messages Via Electronic Communications Networks*[166] in October 2012, which then applied to all mobile network operators in the country.

See: IHRB, *Corporate Responses to Hate Speech in the 2013 Kenya Presidential Elections. Case Study: Safaricom* (2013)

ICTs and the Forthcoming Elections

ICTs have played a key role in sparking democratic movements. Governments have sometimes responded by shutting down all or parts of networks, as happened during the 2007 Saffron Revolution in Myanmar and the 2011 Arab Spring in Egypt. But ICTs have also been implicated in incitement of violence (see Kenya case study, Table 30). Governments in many countries have proposed imposing other restrictions that can have widespread impacts on users.

With elections due in November 2015, social media will facilitate political discourse. While social media have been shown increase a user's exposure to diverse viewpoints[167] in some cases it has been found to do the opposite. A recent study of the diffusion of information over social media for U.S. voters found that "*voters of all groups are disproportionately exposed to like-minded information*".[168] Many social media platforms are designed to surface information that is "relevant *to users*" based on their social media contacts, 'Liked' or 'followed' pages, and reading habits.[169] For example, in a Myanmar context the Facebook followers of controversial monk U Wirathu are most likely Friends or followers of like-minded individuals. This could result in statements classified as dangerous speech (statements which could provoke an emotional response) spreading at a rapid pace. See also Chapter 4.2 on Hate Speech.

Cultural Impacts

Localisation and Access to Information

The successful realisation of positive sector-level impacts ranging from economic growth, e-governance and social inclusion depends on increasing access to information to allow the full range of Myanmar's population to participate in Myanmar's growing 'information society'. To support that participation, ICTs must be localised for Myanmar users. This 'localisation' means adapting technology to support a user's local language and culture.

---

[166] Communications Commission of Kenya, "Guidelines for the Prevention of Transmission of Undesirable Bulk Political Content via electronic Communications Networks" (August 2012).
[167] Pablo Barberá "How Social Media Reduces Mass Political Polarisation: Evidence from Germany, Spain, and the U.S." (October 2014).
[168] Yosh Halberstam, Brian Knight, "Homophily, Group Size, and the Diffusion of Political Information in Social Networks: Evidence from Twitter" (November 2014).
[169] On April 21, 2015 Facebook announced changes to its news feed designed to prioritise content that was relevant to users. See "News Feed FYI: Balancing Content from Friends and Pages" (April 2015).

This includes hardware, software, and educational material or user manuals. It also refers to meeting a user's local needs,[170] which can be achieved through supporting content creation in local languages and offering relevant applications. Content that is relevant to a farmer may be different from content relevant to a younger urbanite. [171]

Inclusive development in the ICT sector will depend on the accessibility of ICTs, beyond functioning telecommunications networks. Users must be able to interact with technology, produce and consume content, and communicate in their local language across a multitude of devices and software. For all services, providing users with the option of interacting with the software's user interface in their local language will support a user's familiarity with managing profiles, accounts, and devices. For social media, this might include translating community standards and instructions on how to use content reporting mechanisms into the local language. Analysis by the International Development Research Centre (IDRC) emphasises that the components of language localisation are interdependent and that localisation extends beyond basic communication, impacting "*matters of culture that are inherently political, economic and social in nature*".[172]

For users in Myanmar, interacting with online services is still a new experience, including how to set up accounts for email and social media services. Around various neighbourhoods in Yangon and Mandalay, street vendors offer to set up individual Facebook and Gmail accounts for new Myanmar users, charging from 1,000 to 5,000 MMK. Currently, localisation debates in Myanmar centres on which type of font to use. There are currently two options available to users: Zawgyi font (commonly used with 'Bagan Keyboard' app for Android phones) and Unicode fonts such as Myanmar 3.

Unicode itself is not a font, but a universal encoding system that enables people around the world to use computers in any language. Fonts themselves can be compliant with the Unicode standard. Unicode features standardised character ordering, which allows for consistent searching in search engines or databases, sorting, and information retrieval across multiple platforms, countries and languages. Outside of Myanmar the majority of websites are also encoded using Unicode (popular examples include Facebook and Wikipedia) and large commercial software and hardware providers such as Apple, Microsoft, and Google now support Unicode in their newest products by default.

Zawgyi is the predominantly used Myanmar language font, but uses a different system to Unicode to encode text to data and data to text. Characters in Zawgyi font can be entered in various ways, creating problems for search and retrieval, whereas Unicode is standardised. If a user does not have Zawgyi font installed on their Android device, they will not be able to read anything typed in Zawgyi. Regardless of the technical benefits of Unicode, the majority of Myanmar users continue to use Zawgyi font based on familiarity.

---

[170] Sarmad Hussain and Ram Mohan, "Localisation in Asia Pacific" Digital Review of Asia Pacific (last accessed August 2015).

[171] See PAN Localisation, "Expanding Digital Literacy through Localized ICTs Experiences of PAN Localization Project 2007 – 2010" (2012), pg 46. The study found that the development and effective distribution of relevant local content,[171] combined with localised ICTs, built digital literacy faster. Researchers in the study noted, "*…After training on localised ICTs, non-users of the computer were not only using the computers for routine tasks but also provided trainings to others*".

[172] Chaitali Sinha & Raymond Hyma, "Connecting ICTs to Development: The IDRC Experience" (2013) p102

While official data on Zawgyi's user base is not available, members of Myanmar's ICT community estimate 75-80% of users in Myanmar type in Zawgyi.

Some members of Myanmar's nascent developer community have opted to offer their applications in English only.[173] Others have taken steps to support broader information accessibility as Myanmar's ICT community migrates to full Unicode support. While Google Translate allows users to input text in Zawgyi, output text is in Unicode. The Myanmar Computer Federation (MCF), an umbrella organisation for computer-related groups and associations, now includes a Zawgyi-Unicode two way conversion tool on their website.[174] Previous attempts to compel users to switch from Zawgyi to Unicode have been unsuccessful when framed as a mutually exclusive choice between the two. However greater migration to Unicode will increase content that is searchable and retrievable through search engines and databases. This will have positive education, transparency and governance impacts.

Supporting Ethnic Language Use and Content

ICTs can positively impact people's ability to access and understand information. But in some cases, it can have the opposite effect. The IDRC notes *"…ICTs can also be used to crowd out minority languages due to content in a dominant language being more readily available and spread."* [175] With over 100 languages spoken in Myanmar, language localisation is essential to ensure all communities have the potential to benefit from new technology. Unicode is a powerful resource, providing support for Shan, Mon and Karen languages.[176] Allowing users to type in their local language enables content creation, which in turn can support users developing familiarity and comfort interacting with ICTs.

Table 31: Language Localisation Challenges in the Danu Community

Myanmar's linguistic context is complex and continuing to evolve, evidenced by the Danu people of Shan State who speak a dialect of Burmese. During MCRB's field research in Shan State, Danu villagers noted that there is on-going debate around alphabet use in the Danu community. Because Danu people do not have their own alphabet, they have adopted Burmese alphabets to teach their children but spellings may vary between Burmese and Danu. Some Danu people are thinking of creating their own alphabet based on old Burmese alphabets dating back to the 16-18 century. In the future, ethnic language support for the Danu language would include keyboards and software to support the newly created alphabet.

While ethnic language fonts are not currently available on the Myanmar Computer Federation (MCF) homepage, MCF now provides links to Myanmar3 (Unicode font) and Pyidaungsu Font (a font package for iOS devices, the operating system designed and

[173] For an example see, Tim Mclaughlin "The Uber of Myanmar" (March 2015).
[174] Myanmar Computer Federation, "Zawgyi – Unicode Conversion Tool" (last accessed August 2015).
[175] See IRDC, "Connecting ICTs to Development: The IRDC Experience" (2013), pg 101.
[176] As an example, Shan Unicode resources are located at http://www.shanunicode.com/.

used by Apple). By highlighting access to these language resources, and MCF's Zawgyi-Unicode conversion tool online, this should benefit users. As the ICT sector grows, there will be further opportunities to direct users to centralised language resources. In Cambodia for example, the Khmer Software Initiative website contains a collection of software, fonts, and resources that can localise proprietary software (such as Windows or Apple OSX) while also providing a variety of localised open source downloads such as Open Office, and Open Suse, a free Linux based operating system.[177]

Social Impacts

Digital Literacy

With SIM cards and entry level Android smartphones costing 1,500 MMK and 50,000 MMK respectively, owning an Internet connected mobile phone is starting to be financially realistic for much of the population. While official data on digital literacy in Myanmar is limited, the increase in mobile penetration over the past 15 years suggests many users are interacting with online services for the first time over an Internet connected mobile phone. A 2014 study by OnDevice Research conducted prior to the commercial launches of Telenor and Ooredoo found that 49% of Myanmar's Internet users accessed the web via a mobile device.[178]

In Myanmar many social interactions are moving to digital venues, such as social media. Many users accessing the Internet for the first time perceive Facebook as 'the Internet'. Myanmar currently has approximately 3.28 million Facebook users, a number that will only increase with additional mobile penetration and Internet access.[179] Messaging and chat applications such as MySquar, Viber, Line, WeChat, and Facebook Messenger are very popular in Myanmar.[180] These applications allow users to send messages over the Internet which is often cheaper than sending an SMS text message between two phones. They offer additional features such as gaming, video calling, online stickers, and media sharing. Viber now incorporates features such as 'public chats' which are conversations anyone can see. Hush, a new mobile application in Myanmar, allows users to post messages and questions that are publicly visible but identify the author only by location.

Digital interactions provide a space for personal expression. But there are significant emerging risks accompanying ICT usage, which new users of Myanmar's growing ICT sector need to be aware of, including responsible social media interaction and managing data privacy online. The ICT Master Plan called for the "*establishment of the National Committee for Information Culture Movement*" to promote e-awareness in Myanmar society. However, to date there has been little action from the Government on promoting e-awareness. Furthermore, Myanmar's education system, which is based on rote learning, rather than critical thinking and analysis, does not generally build the skills

[177] See examples in Cambodia via KhmerOS at http://www.khmeros.info/.
[178] OnDevice Research, "Myanmar: The Final Frontier of the Mobile Internet" (July 2014).
[179] DVB, "Govt, facebook to purge hate speech accounts" (14 Sept 2015).
[180] Myanmar Times, "MySQUAR Aims for Listing in London" (May 2015).

needed to debate the ethics of the complex societal issues which arise from ICTs, and identify appropriate rights-based solutions.

Table 32: A Myanmar Civil Society Initiative on Responsible Use of Social Media

Panzagar (Flower Speech) is a grassroots campaign[181] founded by Nay Phone Latt, Executive Director of Myanmar ICT for Development Foundation (MIDO). Panzagar aims to promote responsible use of social media, and raise awareness of the implications resulting from online behavior. Panzagar has partnered with local graphic designers and Facebook to create a set of 'digital stickers' users can stick in comments or messages online. (See Chapter 4.2 on Hate Speech for further details)

Use of ICT for Exploitation and Degrading Treatment: Cyber Bullying, Online Harassment, Non-Consensual Pornography (Revenge Porn)

While not defined in international law, cyber-bullying refers to bullying that takes place over any electronic technology, including mobile phones, laptops, tablets, and desktop computers as well as online services such as emails, social media, instant messaging, or over a phone call. Cyber-bullying is deliberate and can include threats, insults, or rumours targeted solely at the victim and others to a larger audience online. Cyber-bullying can occur in numerous forms, and the impacts can be severe.[182] An emerging trend in cyber-bullying is called 'doxxing' which refers to the public sharing of an individual's personal identifying information online. In August 2015, Yangon police authorities publicly highlighted that anyone using ICTs to disturb, threaten or defame others in a sexual manner could face penalties of three to five years' jail and/or a fine.[183]

In 2011, a Myanmar woman studying in Singapore committed suicide after her ex-boyfriend posted public comments on her Facebook page accusing her of sexual promiscuity.[184] More recently, other women have reported threats of blackmail online. Blackmailers have threatened to distribute public profile pictures, along with posting degrading rumours online, and demanded mobile top up cards as payment to prevent the posting of personal information.[185] Women have reported receiving lewd photographs from individuals using fake Facebook accounts, who then demand that the women send them nude photographs.

Non-Consensual Pornography (also referred to as 'Revenge Porn') is an emerging risk for Internet users around the world. This form of harassment can occur across ICTs (social media, chat applications, email, etc.) and involves the public distribution of photographs or video that was shared privately between two people. When private intimate content is shared publically, it can often go viral, spreading beyond the original platform it was

[181] For more information on Panzagar see https://www.facebook.com/panzagar and Travelling Panzagar
[182] *ibid*
[183] Myanmar Times, "Cyber sex offenders get time" (10 August 2015).
[184] Asia One, "Ex-boyfriend called her a 'loose woman", (April 2011).
[185] See 7 Day News Print Daily (20 May 2015).

posted to, leaving the victim with limited options for remedy.[186] Major social media platforms have taken steps to address revenge porn. In March 2015 Twitter, Reddit, and Facebook updated their community standards to prohibit the posting of revenge porn.[187] While these moderation mechanisms exist, users in Myanmar may be unaware of how to access them.

Child Safety Online

Children can be particularly vulnerable to digital dangers when using ICTs. This can include cyber-bullying or harassment online, accessing inappropriate content, or sexual exploitation. Children that are targeted online can experience various degrees of trauma that can affect their performance in school, social relationships, and mental health.

Limited information is available regarding the risk of child sexual abuse images in Myanmar, but high levels of poverty combined with improved Internet access poses new risks. There is little evidence that this has been a priority for child protection agencies or NGOs in Myanmar to date, given low Internet penetration levels. This is an area where awareness raising, appropriate standards and stronger penalties will be required. Under Section 66 of Myanmar's *Child Law*, the production or resale of child sexual abuse images can result in maximum fine of 10,000 MMK (approximately US$8) and a two-year prison sentence.[188]

Education

ICTs interact with the education sector in at least three ways:

- *ICT Education* focused on students learning how to program or use software applications and/or training future ICT technicians/experts. See below for the status of ICT Education in Myanmar
- *ICT in education* focused on teachers incorporating ICT into teaching in the classroom, e.g., multimedia classrooms, Powerpoint to support lectures, use of computers for testing or tracking student records, etc). The potential benefits of expanding ICT in primary and secondary education in Myanmar must be carefully assessed against international evidence as well as the high capital and recurrent costs this would impose and the resources this would draw away from other higher impact investments in the education sector.[189]

---

[186] An increasing number of governments around the world are adopting legislation that criminalises revenge porn. To accelerate these efforts, the Cyber Civil Rights Initiative (CCRI) has organised a campaign called End Revenge Porn and published a guide for legislators to assist with the development of legislation that criminalises non-consensual pornography.

[187] For example, Twitter's community standards now prohibits the sharing of private intimate photos or video. See Twitter, "The Twitter Rules" (last accessed August 2015). See also Facebook, ""Community Standards", "Sexual Violence and Exploitation" section, (last accessed August 2015).

[188] Section 4, section 84 (a) of the Myanmar *Child Law*.

[189] See for example, World Bank, "Worst practice in ICT use in education" (2010). As part of Myanmar's Comprehensive Education Sector Review (CESR), a survey of secondary schools nationwide (supported by ADB and Australia) confirms that "hardware-driven" approaches would be hugely costly: e.g., roughly 2/3 of responding rural basic education middle schools had no electricity and no computers, and virtually none had

- *ICT <u>for</u> education* which may include the above, but starts more firmly from the philosophy that ICT is a tool to support education, typically requiring ICT to be strategically combined into broader approaches).

The Status of ICT Education

Accessing ICT-focussed higher education, and technical and vocational education and training (TVET), can be challenging for prospective students. There are 25 Computer Universities in Myanmar. To enter the Technical University system in Myanmar, students must achieve a certain level of 10th Grade matriculation exam marks out of a total of 600. According to 2013-2014 University entrance results, the most competitive subject is Medicine. Access is discriminatory, with male students requiring marks of 490 and female students 508 to gain access[190].

The Yangon University of Computer Studies also requires comparatively high marks (473) compared to other subject areas, as does Mandalay University of Computer Studies (450), but does not discriminate between sexes. These two Universities offer Masters and PhD courses and are better equipped than the Computer Universities in other parts of the country (which generally require around 365 marks). By comparison, Yangon Institute of Economics requires marks of 383; other disciplines e.g. Chemistry, Physics, History require less.

If students do gain access to a Computer University, they can experience further challenges. During a focus group discussion in Mandalay, local stakeholders noted that while there are four Computer Universities in Mandalay Region (two in Mandalay, one in Pyin Oo Lwin, one in Meiktila), the local university system only has enough faculty to adequately staff two. Some professors are forced to split their time between multiple universities, leaving students without support on assignments or projects. Limited human resources, combined with long commutes to universities located outside of the city and a lack of boarding accommodation results in students spending limited time on campus outside of class.

Curriculum in the public Technical University is disconnected from the needs of employers in the sector for several reasons. Stakeholders in Yangon and Mandalay have noted that in technical terms, many aspects of the curriculum are "*ten years behind*". A well-funded Myanmar start-up based in Yangon noted difficulties hiring recent graduates with any experience developing code in newer programming languages such as Ruby on Rails or hiring a qualified iOS developer who had practical experience applying their knowledge outside of the classroom.

In some cases, updated technical training is available through private ICT education offering accredited international courses. But high costs deter the majority of potential

more than 2 computers. The initial capital costs of computer installation would likely, in turn, be eclipsed by various recurrent costs (e.g., electricity, maintenance, upgrading/replacement, etc.).

students. Private education can cost up to $3,000 per year compared to $150 per year at public universities.

To understand the needs of the ICT labour market, collaboration between relevant Government ministries and private sector ICT companies will be required. This involves assessing desired qualifications and expanding opportunities for students to practically apply their knowledge in real-world settings such as business case competitions, or software development events such as 'hackathons'.

Health Services

Organisations in Myanmar are beginning to utilise ICTs, particularly mobile technology, to provide health services. Mobile health (mHealth) applications can be used for remote data collection or monitoring of patients, facilitating information exchange between health care providers, tracking diseases and epidemics.[191] The potential of mobile includes improved access to information for patients and providers, as well as reduced costs.[192]

Ooredoo Myanmar, through a partnership with Population Services International Myanmar and Koe Koe Tech, has launched the 'May May' (Mummy) Android app for pregnant women. The application allows users to receive weekly health notifications and locate doctors nearby. The app also includes an optional social component, through Facebook connectivity. Telenor Myanmar has also partnered with Marie Stopes International Myanmar to launch future mHealth services.[193] In September 2013, core members of the Ministry of Health's national team were trained on DHIS2[194], a powerful free software program for aggregating and analysing health information.[195]

Myanmar currently lacks legislated standards around data collection, data privacy, and data protection. As mHealth programs expand, data collection and privacy will be a major concern, particularly with at risk communities where social stigma exists. Examples of these communities may include men who have sex with men, female sex workers, or other sensitive patient populations such as those with HIV/AIDs. The disclosure of these patients' health information or a data breach could result in harassment, violence, or discrimination. This could further exacerbate challenges surrounding health outreach to these populations.

While mHealth programs are powerful tools for disseminating health information and connecting patients with healthcare professionals, mHealth applications must be adapted for use by ethnic minorities so they can access health information in their local language. Health care providers have typically relied on local health staff to translate local health

[191] See United Nations Foundation, Vodafone Foundation "mHealth for Development: The Oppurtunity of Mobile Technology for Healthcare in the Developing World" (2011), pg 9.
[192] See McKinsey & Co, "mHealth: A new vision for healthcare" (2012) and BCG Perspectives "The Socioeconomic Impact of Mobile Health" (29 May 2012).
[193] See Telenor "Telenor and Marie Stopes announce joint mHealth initiative in Myanmar" (28 July 2014).
[194] Department of Health Planning, Ministry of Health, "eHealth in Myanmar" (December 2013)
[195] For an overview of DHIS2, please visit https://www.dhis2.org/overview.

information.[196] By supporting international technical standards (such as Unicode), health care providers and partner organisations can accelerate technical development and content creation.

Disaster risk reduction

In 2008 – when less than 1% of Myanmar had access to a mobile phone – Cyclone Nargis devastated Myanmar, claiming nearly 140,000 lives and displacing 2.4 million people. There was no early warning system in place in 2008 and the Government of Myanmar was harshly criticised for its response to the disaster. The 2011-2015 ICT Masterplan called for the use of ICTs for pre-emptive disaster response, including the establishment of a national disaster prevention network.[197] It is unclear what progress has been made against the recommendations called for in the 2011-2015 Master Plan.

As Myanmar's telecommunications infrastructure continues to improve, more people will have reliable mobile phone service, presenting a major opportunity to leverage ICTs for disaster reduction and relief, seen most recently in the July 2015 floods[198]. National early warning systems can be designed to function over SMS messaging, voice calls, and mass messaging of weather alerts or evacuation notices through cellular broadcasting. Cellular broadcasting is used for mass-messaging alerts to users in a network area.
Technology companies are also offering services to assist in disaster relief. Both Facebook and Google offer services that can be used to locate people impacted by a natural disaster. Facebook's tool, 'Safety Check', uses location data to identify a user in a natural disaster area. Users can then verify they are safe through the Facebook app, or identify others in the impact area they have verified are safe. Google's tool, 'People Finder' focuses on crowdsourcing information on missing people, which is then shared with responders in the area. While not having developed a specific tool, Viber recently offered free Viber Out (calling from Viber to any phone number in the world) calling in and out of Nepal following the devastating earthquake in Kathmandu. However, any such services need to work with emergency specialists to ensure that privacy protections are built into systems – for example there can be unintended consequences for child safety if information about unaccompanied children is posted online and accessible to all, including traffickers.

Environmental Impacts

Disposal of electronic waste/recycling

Throughout Myanmar, it is common practice to burn trash. The incidence of public or private sector rubbish collection and recycling varies across Myanmar, with some

[196] Asia Pacifc Observatory on Health Systems and Policies, "The Republic of the Union of Myanmar : Health Systems Review", pg 59.
[197] See, MCIT, KOICA, ETRI, "The Followup Project of the Myanmar ICT Master Plan" (2011), pg 122.
[198] 'Officials use social media to fight flood rumours', Myanmar Times, 31 July 2015 and 'Social media drives flood donations, Myanmar Times, 7 August 2015

neighbourhoods being serviced by informal recycling services collecting bottles, scrap metal and paper.

Underdeveloped waste management systems in Myanmar – especially outside of urban areas[199] – are unequipped to deal with electronic waste. Electronic waste (e-waste) can be defined as "*all types of electrical and electronic equipment (EEE) and its parts that have been discarded by the owner as waste without the intention of re-use*".[200] There are some markets, such as Yangon's 28th Street, trading in electronic waste then used to refurbish devices or sold for raw materials. In some cases, supplying these markets can be dangerous for so called 'garbage hunters' or 'pickers' who are involved in the salvage process. In the informal sector, the extraction of valuable materials or components from discarded ICTs is done without proper training or protection, exposing individuals to serious health risks. Mobile phones, tablets, laptops, desktop computers, and other consumer electronics contain a variety of toxic substances ranging from heavy metals (lead, mercury, arsenic, nickel, cadmium) and plastics such as PVC that emit dioxin when burned.[201] Human exposure to these substances can result in damage to the brain, kidneys, and liver, severe allergic reactions, and cancer.

Handset use is increasing. The MCIT hopes to achieve 80% mobile penetration by 2016. With a population of 51.4 million, this would imply over 40 million mobile phone users in Myanmar. This increase in handsets and other ICT equipment will require the development of formal waste management processes for e-waste, including enhanced regulations and training for individuals participating in the informal sector. Estimates by the United Nations' STEP Initiative note that Myanmar generated 29 metric kilotonnes of e-waste in 2014, which excludes any waste that has been exported to Myanmar from other countries.[202]

E-waste can also involve foreign countries shipping their own electronic waste abroad. This trend has been documented in developed countries, where e-waste is often exported to developing countries under the guise of 'recycling' due to weaker environmental regulation, cheap labour, and lack of export controls over sending e-waste abroad.[203] Exported waste can contaminate land and groundwater. Official current data on e-waste exported to Myanmar is not readily available. A 2007 report by the United Nations Environment Programme noted that 90% of the then 20-50 million tonnes generated every year is sent to Bangladesh, China, India, Myanmar, and Pakistan.[204]

Environmental Impact from Towers

Mobile network operators require consistent power to operate their networks, as base transceiver stations (BTS) located at tower sites must be powered on 24 hours a day, 365

[199] Yangon City Development Committee announced the privatisation of trash collection services in 2015, see Myanmar Times "Trash Talk" (15 December 2014).
[200] See STEP Initiative, "What is E-Waste?" (last accessed August 2015).
[201] See Basel Action Network, "Exporting Harm : The High Tech Trashing of Asia" (2002), pg 9.
[202] See Overview of E-Waste Information for Myanmar at www.step-initiative.org/Overview_Myanmar.html
[203] Ibid pg 8. See also, The Guardian "Toxic e-waste dumped in poor nations, says United Nations" (2013).
[204] See, United Nations Environment Programme, "Geo 4: Global Environment Outlook" (2007), pg 225.

days per year. Each tower's power consumption can vary depending on the number of network operators with BTS located at the site. In India, Bharti Enterprises (owner of Bharti Airtel) notes that "*an average mobile tower consumes 96 kilowatts of power daily*" and that in areas where electricity is unreliable "*diesel consumption can average 24 litres per day*". [205] For reference, the World Bank notes that Myanmar's per capita power consumption is 160 kilowatts per year.[206]

Reliable energy access continues to be a major problem across Myanmar. The World Bank estimates that 70% of Myanmar's population lacks access to on-grid electricity,[207] while residents of Myanmar's larger cities where grid power is available continue to experience intermittent power outages due to high demand for electricity.[208] To address the issue of unreliable power, the majority of mobile towers in Myanmar are currently powered by a diesel generator, or by a combination of diesel generator and hybrid electric battery. While both foreign operators allude to sustainable energy usage on their respective websites, specific data regarding current renewable energy usage from Telenor and Ooredoo is not publically available.[209] MPT does not provide information online regarding energy policy, but media reports indicate that in 2014 MPT contracted Vihaan Networks Limited to install 31 solar powered base stations at tower locations located along the Yangon-Mandalay highway.[210]

Outside of renewable energy usage, there are additional opportunities to utilise mobile tower power for community-based micro grids. A Yangon based renewable energy expert notes that excess power produced by the diesel generator (potentially 2-3 kilowatts per day) could be utilised for community power while the diesel generator is running, providing community members with the opportunity to power lights or charge mobile devices through connected micro grids. This model has been adapted in India, where a micro grid connected to 40 towers has provided electricity to 30,000 households.[211] Currently there is no grid feed-in tariff that allows tower operators to sell excess energy capacity to the local community or to energy operators.

The GSM Association (GSMA) estimates power requirements for Myanmar's mobile networks will exceed 455 GWh by 2017, compared with 200 GWh in 2015.[212] Additionally, the GSMA estimates that the annual diesel requirement will reach 116 million litres by 2017, resulting in 310,676 tonnes of annual CO_2 emissions.[213] In addition to CO_2

[205] In India, Bharti Enterprises notes that "an average mobile tower consumes 96 Kilowatts of power daily" See Bharti, "How Mobile Towers are Reducing Carbon Footprint" (last accessed August 2015).
[206] World Bank, "Project Information Document (Concept Stage): National Electrification Project" (Dec 2014).
[207] *Ibid*, pg 2.
[208] The Irrawaddy "Rangoon Power Supplier Blames Rise in Blackouts on High Demand" (May 2015).
[209] Ooredoo Myanmar notes "*As a socially responsible company we are committed to mitigating the environmental impact of our business activities. Using innovative technologies in rural areas we deploy alternative energies to power our tower sites, using solar energy as an alternative to fuel consumption.*" Ooredoo, "Respecting the Environment" (last accessed 25 Aug. 2015). Telenor Myanmar notes it will complete an environmental impact assessment in compliance with Myanmar's *Environmental Act*, and that "*Telenor is committed to minimising CO2 emissions in Myanmar, such as through the use of solar power, and the ambition will thus be to minimise energy consumption."* Telenor "Environment" (last accessed Aug. 2015).
[210] Vihaan Networks Ltd, "Seemless GSM Connectivity for Yangon – Mandalay New Highway" (Feb 2014).
[211] The Economist "Could your mobile phone bring you light, too?" (May 2015).
[212] GSMA, "Seizing the Opportunity: Green Telecoms in Myanmar" (2014).
[213] *Ibid*.

emissions, diesel generators cause localised particulate and noise emissions, noted as a significant issue by community members during MCRB's field research. While fuel theft does not yet seem to be a major problem in Myanmar, as awareness of the availability of fuel at tower sites grows, this could become a challenge in Myanmar as it has in other countries.

In addition to concerns about air and noise pollution, community members also noted concerns about the health risks from mobile towers. In March 2015, the Posts and Telecommunications Department (PTD) held a public forum sharing results from field-testing radiation levels of mobile towers across Myanmar. Findings showed that EMF radiation levels of Myanmar mobile networks were far lower than limits regarded as harmful by the World Health Organisation.[214] PTD also presented a Burmese language information leaflet for community members to be distributed during the tower construction process.[215] It is not, however, clear who is ultimately responsible for distributing the leaflet, PTD, operators or tower companies and their sub-contractors. Some operators have delegated this responsibility to their community engagement teams. Plans around translating the brochure to ethnic languages are currently unclear.

Geographic Information Systems (GIS)

Geographic Information Systems (GIS) refers to specific applications of ICT for geographic and spatial analysis. In GIS, data for a specific area can be layered allowing a user to analyse the spatial relationships. GIS has numerous applications (environmental, human geography, health, urban planning), but depends on the availability of reliable data. This is a particular challenge for Myanmar.

The Myanmar Information Management Unit (MIMU) www.themimu.info is a focal point for GIS activities in Myanmar. It is working to support the development of a National Spatial Data Infrastructure (NSDI). MIMU maintains various data sets on Myanmar (aggregated from INGOs and civil society groups), including data at the township and village level. Additionally, MIMU provides training resources in Myanmar language on open-source GIS software such as QGIS, which can be downloaded for free. Access to such data can provide powerful tools to help civil society organisations understand impacts that have happened and to project forthcoming changes. For example, EcoDev is currently combining satellite images from NASA's LandSat satellite with GIS to map changes in Myanmar's forests over the past decade. This information can be used to hold the Government and private sector to account.

In June 2015 a project called 'OneMap Myanmar' began its inception phase to develop a GIS system compiling, enhancing and making available and accessible union-wide data on land use, land cover and land tenure. It also aims to incorporate valuable data generated locally, including data from civil society organisations. This data can then

[214] See: WHO, "Electromagnetic Fields" (last accessed August 2015).
[215] Posts and Telecommunications Department, "Media Release: Myanmar Government: No Evident of Health Risk from Myanmar Mobile Network" (March 2015)

inform the Myanmar Government's land governance policy decisions.[216] The project is slated to run over eight years, implemented by Centre for Development and Environment (CDE) of Bern University in partnership with Myanmar's high-level Central Committee for Land Resource Management, but with a focal point in the Ministry of Environment Conservation Forestry (MoECAF).

Table 33: Licenses Issued as of August 2015

No.	Issued	Expires	Company Name	License Type
1	5-2-14	4-2-29	Ooredoo Myanmar	*Nationwide Telecommunications*
2	5-2-14	4-2-29	Telenor Myanmar	*Nationwide Telecommunications*
3	30-1-15	29-1-30	Shwe Than Lwin Media	*Network Facilities Service (Individual)*
4	30-1-15	29-1-30	Eager Communications Group	*Network Facilities Service (Class) Application Service*
5	30-1-15	29-1-30	Global Technology	*Network Facilities Service (Class)*
6	3-2-15	2-2-30	Myanmar Fibre Optic Communications Network	*Network Facilities Service (Class)*
7	3-2-15	2-2-30	Pan Asia Majestic Eagle	*Network Facilities Service (Class)*
8	3-2-15	2-2-30	Digicel Myanmar Tower Co	*Network Facilities Service (Class)*
9	3-2-215	2-2-30	Irrawaddy Green Towers	*Network Facilities Service (Class)*
10	3-2-15	2-2-30	Apollo Towers Myanmar	*Network Facilities Service (Class)*
11	25-2-15	24-2-30	KDDI Summit Global Myanmar	*Network Facilities Service (Class)*
12	27-2-15	26-2-30	Elite Telecom Public Co	*Network Facilities Service (Individual)*
13	27-2-15	26-2-30	Yatanarpon Teleport Public Co	*Network Facilities Service (Individual)*
14	23-3-15	22-3-30	Frontiir Company	*Network Facilities Service (Individual), Application Service*
15	23-3-15	22-3-30	Myanmar Economic Corporation	*Network Facilities Service (Individual)*
16	24-3-15	23-3-30	Myanma Posts and Telecommunications	*Nationwide Telecommunications*
17	25-3-15	24-3-30	Digital Communication	*Network Facilities Service (Class)*
18	26-3-15	25-3-30	Myanma Railways	*Network Facilities Service (Class)*
19	3-4-15	2-4-30	Myanmar World Distribution Trading	*Network Service*
20	23-4-15	22-4-30	Myanmar Technology Gateway	*Application Service*
21	23-4-15	22-4-30	Myanmar Network	*Network Facilities Service (Individual)*

[216] University of Bern Centre for Development and Environment, "OneMap Myanmar: New CDE Project Launched" (8 July 2015).

22	27-4-15	26-4-30	Myanmar Padauk Engineering & Construction	*Network Facilities Service (Class)*
23	30-4-15	29-4-30	VOIP Myanmar Group	*Application Service*
24	30-4-15	29-4-30	Myanmar Telecommunication & Technology Services	*Application Service*
25	30-4-15	29-4-30	Horizon Telecom International	*Network Facilities Service (Class)*
26	12-5-15	11-5-30	Myanmar Cyber	*Application Service*
27	9-6-15	8-6-30	Kinetic Myanmar Technology	*Network Service*
28	9-6-15	8-6-30	Active Business Consolidation Services	*Network Facilities Service (Class)*
29	12-6-15	11-6-30	Union Internet	*Network Facilities Service (Individual)*
30	12-6-15	11-6-30	Eco-Friendly Tower Co	*Network Facilities Service (Class)*
31	12-6-15	11-6-30	Yadanarbon Fibre Services Co	*Network Facilities Service (Class)*
32	12-6-15	11-6-30	Be the First Company	*Network Facilities Service (Class)*
33	17-6-15	16-6-30	Myanmar Payment Union	*Application Service*
34	26-6-15	25-6-30	ShwePyiTaGon	*Network Facilities Service (Individual)*
35	25-6-15	24-6-15	KyawZeyar	*Network Service*
36	25-6-15	24-6-15	Thoo Lei	*Network Facilities Service (Class)* *Application Service*
37	6-7-15	5-7-30	FPT Myanmar (from Vietnam)	*Network Facilities Service (Individual)*
38	7-7-15	6-7-30	Chiyoda and Public Works	*Application Service*
39	8-7-15	7-7-30	Trust Net Solutions	*Network Service* *Network Facilities Service (Class)*
40	9-7-15	8-7-30	Myanmar Golden 11 Investment International	*Network Facilities Service (Class)*
41	14-7-15	13-7-30	Fortune International	*Network Facilities Service (Individual)*
42	14-7-15	13-7-30	Asia Mega Link	*Network Facilities Service (Class)*
43	21-7-15	20-7-30	Golden TMH Telecom	*Network Facilities Service (Individual)*
44	21-7-15	20-7-30	Horizon Telecom International (HTI)	*Network Service*
45	4-8-15	3-8-30	Myanmar Telecommunication Network Public Co	*Network Facilities Service (Individual)*
46	4-8-15	3-8-30	G N E	*Application Service Licence*
47	4-8-15	3-8-30	KBZ Gateway	*Network Facilities Service (Individual) Licence*
48	11-8-15	10-8-30	Thanlyin Estate Development	*Application Service Licence*

Source: Ministry of Communication and Information Technology (MCIT), "Licence Issued List" August 2015

Table 34: Principle Companies Operating in the ICT Value Chain

Fibre optic cable	Mobile network operators
Eager Communications Group Ltd Myanmar Fibre Optic Cable Network Company Ltd. (MFOCN)	Myanma Posts and Telecommunications and KDDI Summit Global Myanmar Company Limited (MPT/KSM) Telenor Myanmar Ltd. Ooredoo Myanmar Ltd.
Tower companies	**Internet service providers**
Apollo Towers Myanmar Tower Company (MTC) Irrawaddy Green Towers Eco-Friendly Towers (EFT) Myanmar Infrastructure Group (MIG) Pan Asia Majestic Eagle Ltd.	Myanma Posts and Telecommunications Yatanarpon Teleport Red Link Sky Net Telenor Myanmar Ltd. Ooredoo Myanmar Ltd. Elite Fortune Frontiir
Network equipment providers	**Web based service providers**
Nokia Siemens Networks (NSN) Ericsson Huawei ZTE Wipro	Facebook Google Viber MySquar Bee Chat WeChat Line

Chapter 4

Operational-Level Impacts

4

Chapter 4
OPERATIONAL-LEVEL IMPACTS

In the following Chapters:

The following chapters present the analysis and findings from a range of existing ICT activities in Myanmar, recognising that impacts are often very context-specific and importantly can be avoided or shaped by (good and bad) company practices. The information presented draws from desk and field research in 13 locations across 6 regions where ICT activities are underway.[217]

Each chapter present common operational-level impacts that are relevant to ICT activities, divided according to **10 key issues in Myanmar:**

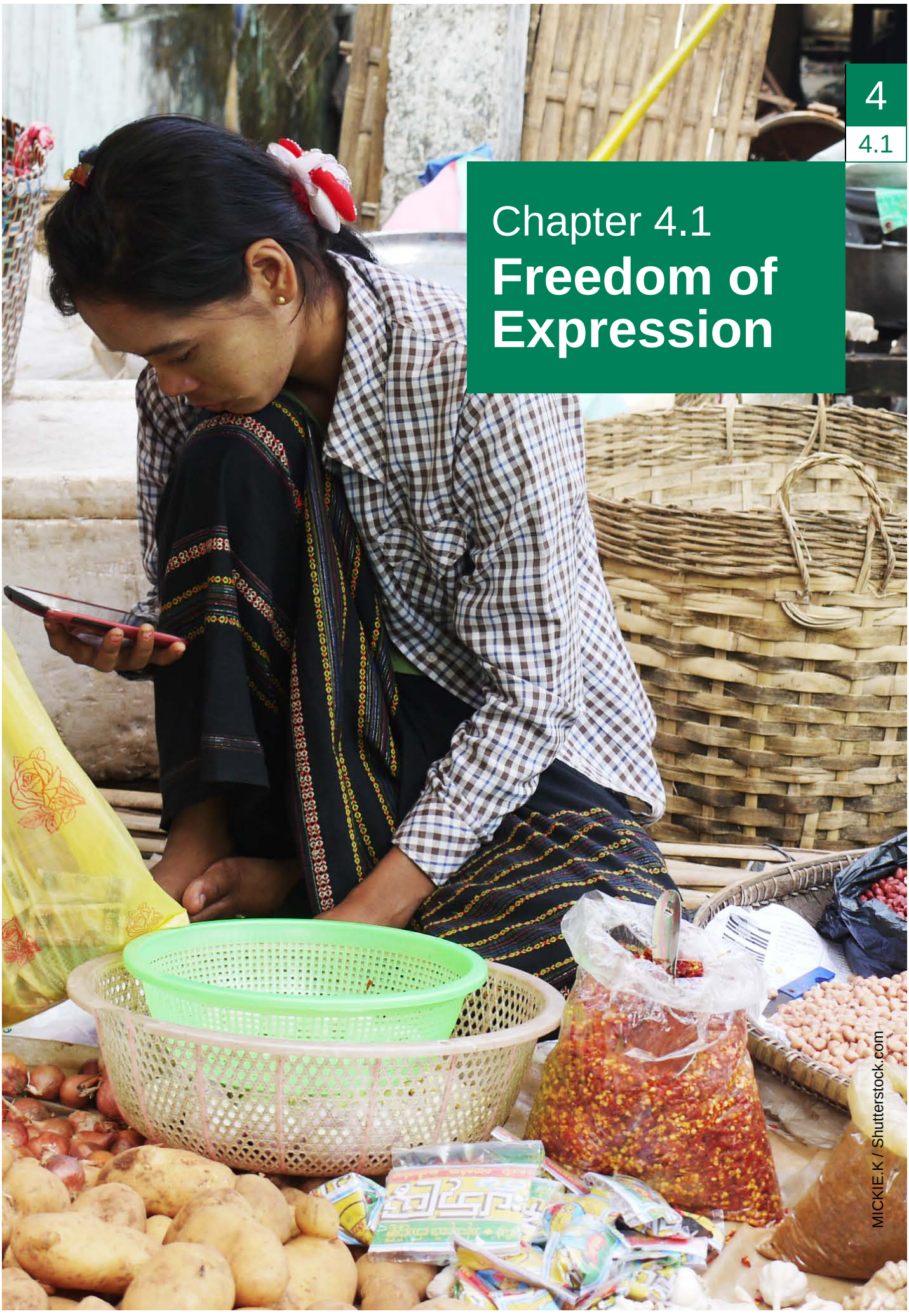
Each Chapter features sections on:

A. Context (national and international)
B. Field Research Findings
C. Recommendations on each of the 10 issues for ICT companies
D. International Standards and Guidance on each of the 10 issues.

MCRB has also published a list of **ongoing 'linked' initiatives** in Myanmar connected to the ICT sector and human rights that it will endeavour to keep updated to provide information on relevant initiatives and potential partners or sources of information for ICT companies.

[217] See Annex A for further information and a map of locations visited.

Chapter 4.1
Freedom of Expression



MICKIE.K / Shutterstock.com

4
4.1

Chapter 4.1
Freedom of Expression

In this Chapter:

A. Context

Freedom of Expression, Opinion and Information and the ICT Sector

Under international human rights law and standards, everyone has the right to hold opinions without interference and the right to freedom of expression, including the freedom to seek, receive and impart information. Technological developments and the growth of the ICT sector means the opportunities to express oneself have likewise grown exponentially. The expansion of the ICT sector has allowed individuals to communicate instantly and at a low cost. It has had a dramatic impact on journalism and the way in which we share and access information and ideas.

However the ICT sector can enable or impede the right to freedom of expression and access to information. For example, ICT companies may be asked by governments to illegitimately restrict online content or media broadcasts, or to hand over information on users and their communications. This censorship of content restricts freedom of expression and opinion. If users feel they are being watched, this can cause a 'chilling effect' on freedom of expression. There is growing concern from global civil society and some companies about this, accompanied by some corporate efforts to push back on Government requests for censorship. This can have positive implications for protecting the right to freedom of expression but also potential negative business consequences by risking formal or informal sanctions[218]. Companies in parts of the ICT value chain play a direct role in facilitating or denying the right to free expression, through the choices they make to allow, block or take down content as outlined in their Terms of Service policies.[219]

[218] See for example the Global Network Iniative and the Telcoms Sector Dialogue, and the UN Global Compact "Human Rights and Business Dilemma Forum: Freedom of Expression, Speech and Opinion" (last accessed August 2015).
[219] See for example, Council of European Union, "EU Human Rights Guidelines on Freedom of Expression Online and Offline" (2014).

Freedom of Expression and Opinion in Myanmar

The opening of the ICT market in Myanmar and loosening restrictions on freedom of expression since the 2011 reforms has meant that people have enjoyed wider opportunities to express themselves, share information and communicate in ways that were previously denied. The choices and rules that companies and the Government make as the ICT sector expands will have significant impacts in future on the right to freedom of expression and access to information. Recognising that Myanmar is starting from one of the lowest penetration rates for mobile or Internet in the world, the Government put ambitious requirements on telecommunications operators to expand coverage[220]. In addition, the World Bank is financing pilot projects to implement localised ICT infrastructure in locations not covered by the commercial operators.[221]

Since the reform process began in Myanmar during 2011, there have been signs of improvement in the rights to freedom of expression. This includes loosening restrictions in law and practice, on the media, and in the right to peaceful assembly and the ability to stage peaceful protests.[222] In August 2012 the Government lifted pre-publication censorship, under which the Government had previously required print media to be submitted for approval and censorship before publication. The authorities have also permitted the publication of independent daily newspapers and allowed exiled Myanmar media organisations to return to the country. Independent Myanmar media report regularly on criticism of the Government by civil society, protest demonstrations, and the authorities' crackdown on such demonstrations.

However, during 2014 journalists faced increased harassment and intimidation, and one journalist was shot dead when he reportedly tried to escape from military custody.[223] Reporting on corruption or the military remains problematic, as shown by the arrests of Unity journalists in July 2014, some of whom were sentenced to years of hard labour for an article on an alleged military weapons factory.[224] While the vast majority of those imprisoned solely for peaceful expression of their views have been released, including journalists, scores remain behind bars and others are at risk of arrest and imprisonment under a number of laws criminalising freedom of expression.[225] Indeed, in February 2015

[220] The government initially set a goal of 80 percent penetration rate by 2016, but adjusted this goal to 50 percent in a May press conference. See Jeremy Wagstaff, "Mobile revolution in Myanmar is on the cards, but too slow for many," Reuters (20 January 2013); Justin Heifetz, "'Beauty contest' for Myanmar's telecoms bid," *Mizzima* (14 May 2013); United Nations (UN) Special Rapporteur on Freedom of Opinion and Expression, the Organization for Security and Co-operation in Europe (OSCE) Representative on Freedom of the Media, the Organisation of American States (OAS) Special Rapporteur on Freedom of Expression and the African Commission on Human and Peoples' Rights (ACHPR) Special Rapporteur on Freedom of Expression and Access to Information, "Tenth Anniversary Joint Declaration: Ten Key Challenges To Freedom Of Expression In The Next Decade" (2010) setting out concerns about differences in access to the Internet..

[221] World Bank "Project Appraisal Document On a Proposed Credit in the Amount of SDR 20.60 Million ($31.5 Million Equivalent) to the Republic of the Union of Myanmar for a Telecommunications Sector Reform Project" (January 2014).

[222] In January 2013 the President abolished Order No. 2/88 of 18 September 1988, which had banned gatherings of five people or more. See: The Republic of the Union of Myanmar President's Office, "Order No. 3/2013" (28 January 2013) and "Order No 2/88".

[223] UN Information Centre, "Statement of the Special Rapporteur on the Situation of Human Rights in Myanmar" Yangon, (16 January 2015). The Committee to Protect Journalists (CPJ) has designated Burma as the 9th most censored country in the world.

[224] See for example, The Irrawaddy, "Burma Resorting to Police State Tactics' in Unity Trial: US Official" (17 July 2014).

[225] Amnesty International "Stop Using Repressive Law against Peaceful Protesters" (15 October 2014).

the UN High Commissioner for Human Rights noted that 10 journalists were imprisoned during 2014 "*under outdated defamation, trespassing and national security laws*".[226]

The right to freedom of expression includes the right to seek, receive and impart information. There is currently no law on freedom of information in Myanmar, although civil society is advocating for such legislation.[227] The Government is making preparations to join the Open Government Partnership, an international organisation that seeks strong commitments from participating governments to promote transparency, fight corruption, harness new technologies and increase participation of civil society to make the Government more open and accountable.[228] In order to join, the Government must meet certain criteria; however, it reportedly scored very low in a 2014 assessment.[229] Moreover a December 2014 Asia Foundation survey found very limited public knowledge about Government institutions and functions, and a low level of social trust.[230]

The Government imposed restrictions on the media during the November 2010 elections, which were widely believed to be neither free nor fair, although such restrictions were eased for the 2012 by-elections. Freedom of expression is thus especially important in the run-up to the General Elections scheduled to take place on November 8th 2015. Journalists and civil society will seek to inform the public about elections procedures, campaigning by political parties, and election results. Myanmar media is receiving training on election reporting and civil society working on electoral issues, and political parties have had several meetings with the Union Elections Commission on codes of conduct, voter registration and other election-related issues.[231] In addition, civil society groups are developing innovative ways to utilise new communication tools, including disseminating information about voter lists[232] and assisting with election monitoring.[233] However, mobile communications have been used in other elections to incite violence (see Kenya case study, in Chapter 3, Table 30).

Telecommunications and ICT policy and law in Myanmar is still in a nascent state and as a result, the Government has not yet addressed other areas that will have impacts on the freedom of expression, opinion and information such as intellectual property, defamation, net neutrality, competition[234] and online anonymity.[235] This means that, for the time being, individual ICT companies will manage these issues according to their own policies or Terms of Service. Of the wide range of actors in the ICT value chain in Myanmar, an increasing number are local start-ups and are likely to have little awareness of relevant

[226] UN OHCHR "Myanmar 'needs urgently to get back on track" Seid (25 February 2015).
[227] Eleven Media "Rights Group Pushes for Freedom of Information Law" (26 January 2015).
[228] Mizzima "Myanmar aims to join the Open Government Partnership", (12 November 2014). See also Open Government Partnership
[229] Myanmar Times "CSOs to give input on Open Government Partnership Bid" (22 October 2014).
[230] Asia Foundation "Asia Foundation Releases Results of Nationwide Myanmar Public Opinion Survey" (12 December 2014).
[231] New Light of Myanmar, "Elections and responsibility of the media" (7 March 2015) and Myanmar Times, "UEC to meet civil society, parties" (13 February 2015).
[232] Irrawaddy "Electoral Education Underway as Batch of Voter Lists is Released" (31 March 2015).
[233] Irrawaddy "Myanmar Civil Society Learns How To Harness ICT At USA 'Tech Camp'" (16 January 2014).
[234] VDB Loi "Myanmar's New Competition Law: A Pitbull or a Paper Tiger?" (8 March 2015).
[235] For a longer explanation of many of these issues, see for example: Special Rapporteur on Freedom of Expression, InterAmerican Commission on Human Rights, "Freedom of Expression and Internet" (2013).

discussions, standards and concerns around human rights issues and the ICT sector and their potential impact on the freedom of expression.

Access to Information in Myanmar

There are a number of different dimensions to 'access to information' — the right to seek, receive and impart information, the availability of services in local languages and the actual availability of service (in terms of intentional shutdowns or restrictions of telecommunications services and the blocking, filtering or takedown of content). Article 19 has identified international best practices for right to information legislation (Table 35).

Table 35: ARTICLE 19's Nine International Best Practices Principles on the Right to Information Legislation[236]

- **Maximum Disclosure:** Freedom of Information Legislation should be guided by the principle of maximum disclosure
- **Obligation to Publish:** Public bodies should be under an obligation to publish key information
- **Promotion of Open Government:** Public bodies must actively promote open government
- **Limited Scope of Obligations:** Exceptions should be clearly and narrowly drawn and subject to strict 'harm' and 'public interest' tests
- **Processes to Facilitate Access:** Requests for Information should be processed rapidly and fairly and an independent review of any refusals should be available
- **Costs:** Individuals should not be deterred from making requests for information by excessive costs
- **Open Meetings:** Meetings of public bodies should be open to the public
- **Disclosure Takes Precedence:** Laws which are inconsistent with the principle of maximum disclosure should be amended or repealed
- **Protection for Whistle-blowers:** Individuals who release information on wrongdoing – whistle-blowers – must be protected

Right to Information/Freedom of Information

The Myanmar Framework for Economic and Social Reforms Policy Priorities for 2012-15 (FESR) contains a clear commitment to both the right to information and the freedom of information, highlighting the need to "*move as quickly as possible to define, legalise and enforce the right to information and to improve citizens' access to information*" and to "*developing an institutional environment for free flow and access to information that empowers civil society*".[237] The FESR also states:

> "*GOM [the Government of Myanmar] intends that citizens are able to participate in the political process and to be well informed about policy decisions, which in turn will improve accountability. GOM has also emphasised cooperation with civil society, as a strong and active civil society is a critical counterpart to a more capable,*

[236] Article 19, *"*The Public's Right to Know*."* Article 19, an international NGO focused on Article 19 of the UDHR on freedom of expression, has also published "A Model Freedom of Information Law".
[237] Myanmar Framework for Economic and Social Reforms Policy Priorities for 2012-15 (FESR), para 114

responsive and accountable state as well as a stronger, more competitive and responsible private sector."[238]

Despite these commitments to "*move as quickly as possible*", there is currently no legislation guaranteeing right to information in Myanmar. The Asian Development Bank (ADB) e-Governance Master Pan emphasises the need for "*inclusive, integrated, and citizen-centric governance*". [239] Legislation guaranteeing a right to information would enhance this objective. Technology can also support citizen engagement and accelerate data collection through 'crowdsourcing', where the public submit information to a central platform which can help solve a particular social issue. For example, people can submit reports on local problems to the council through Fix My Street in the United Kingdom [240] or report updates on water supply availability through Next Drop in India.[241]

Preserving ethnic minority languages online

There are a wide range of languages spoken in Myanmar. There is concern that with the concentration of services in English and the predominant language Burmese, other languages will be increasingly marginalised in the online environment. Stakeholders from minority language groups may already be disadvantaged in relation to the physical accessibility of ICTs in their area, given that many of the ethnic minority groups live in the more remote areas of the country, further from the commercial and political capitals.

Denial of Access to Information – Restrictions, Blocking and Removing Content

Regulations restricting Internet usage in Myanmar can be traced back to January 2000 when the Government attempted to restrict the creation of webpages, sharing of Internet accounts, and posting of political content.[242] Research by the Open Network Initiative (ONI) indicates that the partial nationalisation of Internet service provider (ISP) Bagan Cybertech in 2004 was followed by further content censorship online, including the blocking of websites featuring content related to political opposition or human rights (including independent media websites), and the websites of email service providers.[243] Other services have also been briefly blocked to try to protect State telecommunications revenue, including GoogleTalk and Gmail in 2006 and Skype in 2011.[244]

In 2012, ONI conducted a test of blocked URL's on the ISP Yatanarpon Teleport. The results showed a drastic reduction in the amount of content filtered or blocked compared to previous testing in 2005. The categories of content blocked were: Pornography, content relating to alcohol and drugs, gambling sites, sex education, online dating sites and gay and lesbian content. Internet censorship circumvention tools were also blocked. A much smaller amount of content in the 'Political' category was blocked. Almost all of the

---

[238] *Ibid*.
[239] ADB/InfoSys, "Republic of the Union of Myanmar: Design of e-Governance Master Plan and Review of Information and Communication Technology Capacity in Academic Institutions " (July 2015), pg 35.
[240] See: https://www.fixmystreet.com/
[241] See: http://nextdrop.org/
[242] BBC News Online "Burma Clamps Down On The Web" (20 January 2000).
[243] Open Network Initiative, ""Internet Filtering in Burma in 2005: A Country Study" (2005)
[244] Irrawaddy "Junta Blocks Google and Gmail" (30 June 2006) and DVB, "Internet Calls Banned As Junta Loses Out" (20 March 2011).

websites of opposition political parties, critical political content, and independent news sites previously found to be blocked were found to be accessible during 2012 testing.[245]

More recently, as the ICT sector has developed and more international services are available, these services are beginning to track and report on requests from the Government of Myanmar. The social networking site Facebook noted in its Government Requests Report that, in the period July-December 2014, the company restricted access to 5 pieces of content reported by the President's Office based on sections 295(A), 298, 504, and 505 of the Myanmar Penal Code, which covers "*Acts or words which intentionally cause outrage or wound religious feelings" and "Statements or insults which intentionally provokes a breach of the peace or causes public mischief*." [246] (See Chapter 4.2 on Hate Speech).

Network Shutdowns

Fulfilment of the right to access information also relies on the availability of telecommunications services, including mobile services and the Internet. Clause 77 of the *Telecommunications Law* grants MCIT the ability to "*temporarily suspend a telecommunication service, stop or prohibit any type of communication or use of telecommunication services*" when doing so would be "*for the benefit of the people*".[247] The lack of a clear legal framework puts mobile operators, and Internet Service Providers (ISPs) at substantial risk of being ordered to shutdown networks or services without clear legal justification, impacting their responsibility to respect human rights such as freedom of expression.[248]

Network shutdowns are regularly used by governments worldwide to stifle free expression by cutting off the means of delivering a message.[249] As more and more people become connected and rely on mobile and Internet services in their day-to-day lives, Government-ordered network and service disruption become increasingly disruptive and dangerous (see Table 36). Blocking of services during protests also impacts freedom of association, and often precedes further human rights violations.

Myanmar experienced a major Internet disconnection during the Saffron Revolution. In August 2007, protests grew throughout the country in a response to deteriorating economic conditions and political discontent. ICTs facilitated the flow of information from citizen journalists to media outlets around the world. [250] In an attempt to prevent information reaching media outside of Myanmar, particularly regarding police brutality and

[245] Open Network Initiative "Update On information Controls in Burma (23 October 2012).
[246] Facebook "Government Requests Report: Myananmar July 2014-December 2014" (accessed Aug 2015).
[247] *Myanmar Telecommunications Law*, Clause 77.
[248] IHRB, "Network Shutdowns in the DRC: ICT companies need clear rules" (19 Feb 2015).
[249] In 2013 and 2014 alone, Freedom House reported network disconnections, that were likely government-ordered, in Ethiopia, Iraq, Kazakhstan, Pakistan, Syria, Sudan, Uzbekistan, Yemen and Zimbabwe. See Freedom House, "Freedom on the Net" (2014). In Jan 2015, the government of the Democratic Republic of Congo ordered a near country-wide mobile network shutdown following protests over the President's unconstitutional decision to remain in power for a third term. In May 2015 in Burundi, following similar protests over the President's plan to seek another term, the government blocked access to Facebook, Twitter, Viber and WhatsApp. See IHRB, "Network Shutdowns in the DRC: ICT companies need clear rules" (19 Feb 2015).
[250] For further analysis see: Berkman Centre for Internet and Society, "The Role of the Internet in Burma's Saffron Revolution" (28 September 2008).

the killing of protesters, the Government responded by shutting down Internet and mobile phone service. At the time Internet services provided by both MPT and Bagan Cybertech went down from September 29 to October 4, 2007. This was followed by a partial shutdown from 4-12 October during which access was restricted to late night hours between 22:00 and 04:00.[251]

Table 36: Impacts of Government-Ordered Shutdowns or Service Disruptions

The impacts on human rights, the economy and national and personal security during network and service disruption can include:

- Restrictions on freedom of expression and access to information that may not be legal, necessary or proportionate.
- Injured people are unable to call emergency services, and emergency services are unable to communicate and locate people.
- People are unable to assure friends and relatives they are safe, causing panic.
- People are unable to call for help to be rescued from areas where protests are happening.
- Authorities are unable to disseminate important information to move people to safety, or to calm a concerned population.
- Human rights groups are unable to monitor situations effectively.
- Small businesses are unable to operate and livelihoods are affected. For example, businesses are unable to access data held in the cloud.
- Mobile banking transactions, relied on by millions of people, cannot take place.
- Transmission of health information on mobile phones also cannot take place.
- Students cannot access educational material.
- Doctors/ health workers are unable to access research or communicate in real time with each other.
- Other popular services carried out via mobile communications such as voting and birth registration are disrupted.
- Other services dependent on radio network may be disrupted e.g. cashpoints (ATM), public transport information.
- In national security emergencies, functioning communications are essential for an effective lawful interception system to help law enforcement locate and track people planning terrorist activity, subject to the process of law, court authorisation and sufficient oversight.
- Crimes cannot be reported to police via mobile phone.
- Hostages are unable to communicate with police.

More recently, Myanmar's Internet access went down for 1 hour and 19 minutes on 5 August 2013. Given its proximity to the anniversary of the 1988 uprising, there was speculation that the outage was intentional, though officially attributed to a damaged fibre optic cable near the SEA-ME-WE 3 submarine cable landing station in Pyapon.[252]

[251] Open Net Initiative "Pulling the Plug: A Technical Review of the Internet Shutdown in Burma" (2007).
[252] Irrawaddy "Burma's Internet Delays Continue Ahead Of 88 Uprising Anniversary" (5 August 2013).

Table 37: Key points for legislation on Network Shutdown to demonstrate a shutdown is necessary and proportionate

- Network shutdowns impacting the entire country should not be authorised.
- A shutdown must only be invoked if there is a real and imminent threat to national security or a national emergency, and a request must specify the reason for the shutdown.
- These situations must be prescribed by law, including which bodies or agencies are authorised to make a network shutdown request.
- A shutdown request must be approved or authorised by the highest level of the government.
- There must be a clear request process, with limited actors allowed to make the request to operators, and a designated person in the operator to receive the request.
- The shutdown request to the network operators must be in writing.
- The request must specify the duration and geographical reach of the shutdown, and demonstrating direct material necessity.
- Shutdowns should be limited in duration and geographical area.
- Where possible, the public must be informed of the shutdown, the duration, geography and services affected.
- Each shutdown must be logged/recorded, and a list published annually.
- The public must have access to emergency services.
- The legislation must be subject to review, including a review of each shutdown by an independent oversight body.[253]

The impact of network shutdowns on freedom of expression is so severe that Special Rapporteurs on freedom of expression from the United Nations (UN), the Organisation of American States (OAS), the African Commission on Human and People's Rights and the Representative on freedom of the media from the Organisation of Security and Co-operation in Europe (OSCE), have all concluded in a Joint Declaration that cutting off access to the Internet can never be justified under human rights law, including on national security grounds:

> "*Cutting off access to the Internet, or parts of the Internet, for whole populations or segments of the public (shutting down the Internet) can never be justified, including on public order or national security grounds. The same applies to slow-downs imposed on the Internet or parts of the Internet.*"[254]

In a second Joint Declaration, they concluded that shutting down entire parts of communications systems (mobile and Internet) during times of conflict can never be justified under human rights law.

> "…*using communication 'kill switches' (i.e. shutting down entire parts of communications systems)… are measures that can never be justified under human rights law.*" [255]

[253] See IHRB, "Corporate Responses to Mobile Network Shutdowns. Case Study Telenor Pakistan" (*forthcoming*).

[254] *Joint Declaration on Freedom of Expression and the Internet* (2011), Article 6b.

[255] *Joint Declaration on Freedom of Expression and Responses to Conflict Situation* (2015) Article 4c

While these statements cover Internet shutdowns and network shutdowns in conflict situations, there is ambiguity as to the impact of mobile shutdowns in a Government proclaimed 'emergency'.

The Government of Myanmar has an opportunity for leadership in this area by committing to a 'no shutdown' policy, and only taking control of telecommunications networks in the most urgent of circumstances, for example a natural disaster of the scale of Cyclone Nargis that hit the country in 2008 where control of the network may be necessary to organise rescue operations. Table 37 identifies key points for legislation on network shutdown which could underpin such a 'no shutdown' commitment.

Anonymity Online

The issue of anonymity when communicating on the Internet is a contentious area that splits expert opinion. One view holds that people should be identifiable and therefore responsible for what they express, speak, or post on the Internet, as online anonymity can be abused in order to bully or 'troll' others and target and exploit children. In addition, online anonymity permits State officials to assume false identities in order to spy on minority groups, for example gay rights activists on social networking websites. Therefore, it is right that online service providers insist on users registering accounts with their real name and if the name is found to be fake, the account could be removed.

The other view holds that in many countries, those who express themselves openly face severe consequences if they are found out, and they have legitimate reasons to conceal their identity. Journalists, human rights defenders, trade union leaders, opposition politicians, dissidents, whistle-blowers, and other activists fall in this category. Using pseudonyms to protect identity is a practice that pre-dates the Internet. Journalists have long used assumed names when exposing injustice or speaking out against authoritarian regimes, a practice deemed necessary in order to protect freedom of expression. Human rights law does not require people to reveal their identities, and drawing from that, it is not necessary for Internet users to communicate only using their real name. Requiring people to register and provide their personal information to authorities can have significant consequences in certain societies and it can create a 'chilling effect' on freedom of expression.

The MCIT issued draft regulations on the registration of SIM cards, which could have had the same effect through requiring SIM card owners to register personal information. No final regulations appear to have been issued. (See Chapter 4.3 on Privacy).

International Human Rights Law on Freedom of Expression

The Universal Declaration on Human Rights (UDHR) (Art. 19) and the International Covenant on Civil and Political Rights (ICCPR) (Art. 19) are the main international instruments that states commit to regarding the protection of freedom of expression.

Freedom of speech and expression carries with it special duties and responsibilities and is not absolute.[256]

Legitimate Restrictions on the Right to Freedom of Expression, Opinion and Information

Article 19(3) of the ICCPR provides that freedom of expression may be subject to certain restrictions which are: "*a) For respect of the rights or reputation of others; or b) For the protection of national security, or of public order (ordre public) or of public health or morals*." Any restrictions must pass a three-part, cumulative test which should assess whether they:

i. are provided for in national law which is clear and accessible to everyone (principle of legal certainty, predictability and transparency)
ii. have a legitimate aim or purpose, i.e. one of the purposes set out in Article 19.3 (principle of legitimacy), and
iii. are necessary and proportionate to the legitimate aim pursued, meaning that the restrictions must the least restrictive means required and justifiable (principles of necessity and proportionality).

The Myanmar Legal Framework and its Current Application

2008 Constitution

The right of citizens "*to express and publish freely their convictions and opinions*" (Article 354 (a)) is guaranteed by the 2008 Constitution, but with significant restrictions. Article 354 guarantees the rights to freedom of expression, peaceful assembly, and association; however exercising such rights must not contravene "*community peace and tranquillity*". These are very broadly and vaguely worded exceptions that could be (and have been) used to justify infringements to the guaranteed right that go well beyond the high bar imposed under international human rights law to justify restrictions on the freedom of expression.[257] Moreover, the right to freedom of expression is only guaranteed for Myanmar citizens.

Laws Enacted Before 2011 and Still In Force

Many laws that greatly restrict freedom of expression and peaceful assembly have not been repealed and the authorities continue to use them to arrest and imprison people for peaceful activities. These include, but are not limited to:

- 1908 Unlawful Associations Law
- 1950 Emergency Provisions Act
- 1923 Official Secrets Act
- Various articles of the Penal Code, especially Article 505(b)[258]

Before the reform process began, the vaguely worded provisions of the *1950 Emergency Provisions Act*, particularly Article 5, were most frequently used to sentence people to long

[256] See UN Human Rights Committee, "General Comment 34: Article 19 - Freedoms of opinion and expression" (11 September 2011).
[257] Legal Background paper commissioned for IHRB.
[258] For a discussion of these and other laws, see Amnesty International, "Justice on Trial" (July 2003).

terms of imprisonment solely for the peaceful expression of their views. Article 5(e) provides for a maximum sentence of seven years for spreading "*false news*", which is not sufficiently defined as required under international human rights standards to provide sufficient certainty. Article 5(j) provides for the same sentence for disrupting "*the morality or behaviour*" or "*the security or the reconstruction of the stability of the union*", also not sufficiently defined. International human rights standards require that all criminal laws are precise, so that people understand what conduct is prohibited, and can govern their conduct accordingly. Use of vague laws is open to abuse through criminalising conduct that is not understood as criminal before the event. Although the 1950 Emergency Provisions are currently used less frequently, they remain in force.

The *1908 Unlawful Associations Act* has also often been used in the past to imprison peaceful critics of the Government (see Chapter 2 for details).

The *1923 Official Secrets Act* has been used to sentence peaceful critics of the Government, sometimes along with other laws criminalising the rights to freedom of expression and association. Article 3 provides for 3 to 14 years' imprisonment *"(1) If any person for any purpose prejudicial to the safety or interests of the State…"* obtains or communicates information which might be useful to an enemy. "*The interests of the state*" is too broad and allows for the imprisonment of people with information that is not in fact a threat to the security of the State. Other provisions of the law provide for 2 years' imprisonment for anyone who receives, possesses or passes on official information deemed to be secret (Section 5).[259] In July 2014 five journalists from the weekly journal Unity were sentenced to 10 years, later reduced to 7 years, under the provisions of the *Official Secrets Act*, for a story on an alleged suspected military chemical weapons plant on seized land.[260]

Chapter XXI of the 1861 Penal Code, which derives from the British colonial era, provides for punishments of up to two years' imprisonment and/or a fine for defamation. Chapter VII(B), 130(B) provides for punishments for libel against foreign powers.[261] In December 2013 a journalist from Eleven Media was sentenced to three months' imprisonment on charges of trespass, abusive language, and defamation for reporting on a corruption case involving a local lawyer in Loikaw, Kayah State.[262] In March 2015 two journalists from the Myanmar Post were sentenced to two month's imprisonment each on charges of defamation against a military MP in the Mon State Parliament.[263]

Section 505(b) of the Penal Code is currently one of the most commonly used provisions to arrest and sentence people, often along with other laws, for peacefully expressing their views. In October 2014 two activists from the community-based Movement for Democracy Current Force were sentenced to two years' imprisonment under Section 505(b) in reference to a letter written about the need for an election of an interim government. Section 505(b) provides for imprisonment for anyone making, publishing or

[259] Amnesty International "Myanmar: Justice on Trial" (July 2003) pg 28-33.
[260] Human Rights Watch, "World Report" (2015).
[261] *Myanmar Penal Code 1861*
[262] Human Rights Watch "Burma: Repression Marks Press Freedom Day" (3 May 2014).
[263] The Irrawaddy "Journalists Handed 2-Month Prison Sentences on Defamation Charge" (18 March 2015).

circulating information which may cause public fear or alarm, and which may incite people to commit offences "*against the State or against the public tranquillity*".[264]

The *2004 Electronic Transactions Law* (the ETL) creates a range of offences for online content that are much broader than in the criminal code.[265] In addition, the law does not provide safeguards for the right to freedom of expression. Under Article 33 of the ETL, it is a criminal offence to do any act or to receive, send or distribute any information detrimental to a wide range of broadly defined interests: the security of the state, the prevalence of law and order or community peace and tranquillity, national solidarity, the national economy or national culture that go far beyond permitted restrictions to the freedom of expression under international law. These same provisions are replicated in the *Computer Sciences Development Law.* See Chapter 2 for more details.

Laws Enacted Since the 2011 Reform Process

The *Media Law* and the *Printing and Publishing Law*, both of which apply to print and Internet publications, were passed in March 2014. The vague provisions of the *2014 Printing and Publishing Law* and broad powers of a Government Registrar to grant or revoke publishing licenses, led to fears of press self-censorship.[266] However the *2014 Printing and Publishing Law* still represents a step forward compared to the repealed 1962 *Printers and Publishers Law*, which provided for wide censorship powers and imprisonment for operating without registration. Article 8 on content restrictions is broadly worded; for example, although the restriction on "*public order*" is a recognised legitimate objective under international human rights law to justify restrictions on freedom of expression, the law should be much more specific as to what types of statements are being prohibited.[267]

Articles 3 and 4 of the *2014 Media Law* guarantee respectively freedom from censorship and freedom to criticise the Government, but both must comply with the constitution (Article 3(a)), which itself has significant restrictions on freedom of expression. The *2014 Media Law* grants a media council, which is not independent from the Government, unrestricted control to regulate broadcast, print and Internet-based media, including on ethics.[268] However these laws have not – yet – been applied to prosecute users of Internet services such as social networking.

---

[264] Amnesty International "Activist organization targeted again" (6 November 2014).
[265] Article 19, "Background Paper on Freedom of Expression in Myanmar" (2014), pg. 47.
[266] The Irrawaddy, "Burma Clampdown Gathers Pace as Legislation Passed" (17 March 2014).
[267] Article 19 "Myanmar: Printing and Publishing Law, Legal Analysis" (November 2014). See also PEN International, PEN Myanmar, PEN Norway, PEN American Center and MIDO "Contribution to the 23rd session of the Working Group of the Universal Periodic Review. Submission on the Republic of the Union of Myanmar" (23 March 2015).
[268] Article 19 "Myanmar: News Media Law, Legal Analysis" (July 2014) and an unofficial translation of the *Media Law*.

B. Field Research Findings

Freedom of Expression

Human Rights Implicated: Freedom of expression and opinion

Field Assessment Findings

- Many interviewees felt that **reference to the impact of behaviour resulting specifically from ICTs is currently excluded from existing laws** and regulations impacting freedom of expression in Myanmar.
- Interviewees highlighted a **lack of guidelines** across public and private institutions **on how to use social media** appropriately.
- Most interviewees felt that **monks were in positions of particular prominence and power** regarding their influence on public opinion and the messages they convey. They felt monks' sermons were generally abided by without question by their followers.
- Some interviewees **questioned the effectiveness of some service provider's 'real names policies'** in Myanmar as often people open many social media or other online accounts under fake names.
- Many interviewees wanted to see **educational campaigns and programmes** introduced by the Government, on TV/media, and in Myanmar schools on the impacts of **dangerous speech and the need for respect and tolerance.**
- Many interviewees **did not report online speech and content they found offensive to site administrators** because they **did not know this was possible** and **because Internet connection was too slow**. (See Chapter 4.2 Hate Speech)
- Although **filtering of online content** appears to have reduced, BlueCoat network equipment[269] (used for filtering) was observed in one ISP's data centre. While this equipment was noted as legacy hardware pre-2011, it was unclear who had access to the equipment in the data centre. Any formal process around managing requests to block or filter content was unavailable, as was a mechanism to communicate with customers regarding impacts of such requests on them.

Freedom of Opinion

Human Rights Implicated: Freedom of expression and opinion

Field Assessment Findings

- Some **clear tensions** were observed by researchers **between traditional Myanmar culture and the introduction of more modern or global cultural trends via ICTs**.
- **Many interviewees felt that women were more vulnerable to impacts** on their 'dignities' from others' behaviours online and needed to be protected or limited from such exposure.
- Researchers also received **many reports of users believing all information published online was true** and not yet understanding how social media and other platforms worked.

[269] See: CItizenLab, "Behind Blue Coat: An update from Burma" (29 November 2011).

Freedom of Information

Human Rights Implicated: Right to information

Field Assessment Findings

- Access to information has been a challenge in Myanmar for decades. **Many interviewees wanted the Myanmar Government and media to use ICTs to communicate to Myanmar people much more widely, particularly in rural regions**, and felt the introduction of the Internet and mobile technology would dramatically improve their ability to access information.
- Interviewees called for the establishment of **information centres** in rural areas to distribute information and act as knowledge resource hubs where people could seek information.

See also the Field Research Findings in Chapter 4.2 on Hate Speech.

Myanmar Good Practice Examples:

- One of the international licensees is committed to developing 200 community information centres. The aim of these is to foster user adoption of mobile services and digital literacy across Myanmar, to connect to the outside world for rural communities that traditionally have not had access to connectivity or the masses of information available online and boost user adoption of mobile connectivity and Internet in rural areas and improve digital literacy through nationwide initiatives for schoolchildren.[270]
- One company has reported that its Myanmar operations are governed by a Code of Conduct and Code of Business Ethics, covering land, labour, health and safety, the environment, anti-discrimination, and privacy/freedom of expression. It conducted a human rights impact assessment in 2013, which identified key risks that will be reflected in its management systems.[271]
- One company reported that it had no formal establishment, no manufacturing and no direct investment in Myanmar but does sell its products via its network of distributors. They initiated a human rights impact assessment prior to their market entry into Myanmar. It has a Global Human Rights Statement, applicable to Myanmar.[272]

C. Freedom of Expression: Recommendations for ICT Companies

- **Understand conflicts between national and international law:** Myanmar's laws on freedom of expression are not aligned with international laws and standards on freedom of expression. In addition, some clauses in the *Telecommunications Law* may allow censorship and surveillance (see Chapter 2). The World Bank has committed to carrying out a due diligence review of Myanmar's telecommunications laws as part of its Telecommunications Sector Reform project, but to date, none of the reviews have been made public.[273] Recent Government practice has indicated that the

[270] Telenor, "Telenor opens doors of Community Information Centre" (20 November 2014).
[271] Ericcson, "Response by Ericsson: Myanmar Foreign Investment Tracking Project", *Business & Human Rights Resource Centre* (last accessed September 2015).
[272] See further: Microsoft, "Response by Microsoft: Myanmar Foreign Investment Tracking Project", Business & Human Rights Resource Centre (last accessed September 2015).
[273] M. Igoe, "Is Myanmar ready for a telecommunications revolution?" (6 May 2014).

Government at various levels, from local to national, continues to apply the laws and at times draconian practices against journalists, protestors and human rights defenders exercising their right to freedom of expression. These actions risk implicating companies in contributing to these violations when companies are requested to comply with Government requests to take down content, block access, or turn over information.

- **Publicly commit to respecting freedom of expression:** Given these concerns, and the gaps in other areas of law relevant to the sector, companies operating in the sector will need to develop their own policies and procedures to ensure that they are meeting their responsibility to respect human rights. In line with the UN Guiding Principles on Business and Human Rights, companies should make their policy commitment to respecting human rights publicly available.[274] For some parts of the ICT value chain, the policy could provide more specific commitments on issues such as Government requests for data, censorship requests, illegal surveillance, or network shutdowns, including procedures for how to narrow requests that may be disproportionate or challenge requests not supported by law.[275] Further internal procedures setting out how the company will deal with Government requests would be an appropriate precautionary measure to put in place in Myanmar.[276]
- **Take positions on key concerns:** Speaking up in public as an individual company to respond to concerns about censorship or imprisonment in violation of the freedom of expression may be sensitive in Myanmar. But companies might seek opportunities through other means, such as industry associations, embassies, in collaboration with civil society, to express their concerns and convey the impact that the lack of rule of law has on willingness to invest in the country and the risks posed to companies. [277]
- **Collaborate with and learn from other ICT companies:** Companies operating in the sector can look to multi-stakeholder initiatives such as the Global Network Initiative (GNI) and other sources of guidance[278] for principles and guidance on dealing with challenges of being asked to comply with requests that violate human rights. They can also look to the example set by telecommunications operators in Myanmar that have publicly committed to pushing back on Government requests for surveillance until regulations are put in place. These commitments set important precedents for other companies and important signals to the Government on how requests that may violate the right to freedom of expression will be dealt with.
- **Build business partners' capability:** Many of the companies operating in the ICT value chain in Myanmar will be small companies, and many small local companies

[274] Numerous companies operating in the ICT sector have already developed policy commitments on human rights and made those publicly available. See for example the ICT companies among this list: http://business-humanrights.org/en/company-policy-statements-on-human-rights

[275] See: Human Rights Watch "Reforming Telecommunications in Burma: Human Rights and Responsible Investment in Mobile and Internet" (2013).

[276] See: European Commission, "ICT Sector Guide on Implementing the UN Guiding Principles on Business and Human Rights" (2013), pg. 44-46, 59-60.

[277] This is done in other markets for example, the Global Network Initiative has been particularly active in commenting on the need for reform by a range of governments to bring their laws and practices into line with international human rights standards.

[278] The GNI Principles on freedom of expression state that: "*Participating companies will respect and protect the freedom of expression of their users by seeking to avoid or minimise the impact of government restrictions on freedom of expression, including restrictions on the information available to users and the opportunities for users to create and communicate ideas and information, regardless of frontiers or media of communication. Participating companies will respect and protect the freedom of expression rights of their users when confronted with government demands, laws and regulations to suppress freedom of expression, remove content or otherwise limit access to information and ideas in a manner inconsistent with internationally recognised laws and standards*." See also, European Commission, "ICT Sector Guide on Implementing the UN Guiding Principles on Business and Human Rights" (2013).

may have had little exposure to discussions or concerns around freedom of expression and other human rights issues and their role and responsibilities. There is a clear need for further awareness raising and training that could be taken on by business partners, donors, and civil society. ICT companies may therefore find it necessary to put in place contractual requirements and follow up to ensure that their business partners are aligned with their human rights approach.

- **Prevent and mitigate impacts around the 2015 national elections:** Mobile operators and social media providers should consider experiences from other countries (see Table 30 case study on Kenya). They should consult relevant experts and other stakeholders, and devise appropriate responses to a range of pre and post-election scenarios to ensure that they are prepared to deal with unfolding events in a manner that best protects users.
- **Promote and preserve Myanmar languages online:** Companies may want to think creatively or collaboratively with other stakeholders (such as civil society or donors) about opportunities to facilitate access and use of minority languages. Companies should publish Terms of Service in local languages.
- **Understand what is being posted or discussed publicly in online company portals**: The wide range of languages in Myanmar has implications for those companies hosting content, such as social media pages, to be able to understand and decide upon whether content is consistent with the right to freedom of expression and in line with the company's terms of service. See also Chapter 4.2 on Hate Speech.
- **Review anonymity policies**: Companies should think through the implications of including 'real names' policies, and whether these are effective in the context of Myanmar (see Chapter 4.2 on Hate Speech). Companies should err on the side of allowing the use of pseudonyms particularly to individuals or groups who have a well-founded fear of possible prosecution. At the same time, companies may be required by law in some instances to reveal the identity of the user to the State (such as during an investigation into terrorism charges). In such a case, where appropriate, companies should inform the user that his or her identity has been compromised.
- **Provide and publish guidelines for employees and workers on the use of social media.** All companies should publish specific guidelines that educate staff on how to use social media and the Internet responsibly while at work.
- **Raise awareness** of how to use, why to use and the results of using social media platforms' 'content reporting' functions.
- **Promote public awareness of the link between ICT and human rights.** This can encourage more CSOs and media to understand and cover the issues.

Companies can also take steps to promote **access to information**:

- **Be transparent around ICT licenses, contracts and their Terms:** While the process to license the telecommunications operators was more transparent than previous bidding processes in Myanmar, the Government did not make the terms of the licenses public. Few governments do provide transparency around the terms of telecommunications operating licenses, but the pressure for contract transparency and information on tariffs, fees and proceeds around public service contracts will continue to grow. The International Finance Corporation (World Bank Group) "*encourages*" the disclosure of information around telecommunications projects it finances.[279]

[279] IFC "Policy on Environmental and Social Sustainability" (2012), para 53: "*When IFC invests in projects involving the final delivery of essential services, such as the retail distribution of water, electricity, piped gas, and telecommunications, to the general public under monopoly conditions, IFC encourages the public disclosure of information relating to household tariffs and tariff adjustment mechanisms, service standards,*

- **Publicly report on Government requests for censorship:** Transparency enables governments and companies to demonstrate whether they are upholding key human rights principles and for other stakeholders to hold governments and companies accountable to such principles.[280] A key development in company transparency in the ICT Sector has been the annual or bi-annual release by some companies of information relating to Government requests companies receive for content takedown, or requests for user data.[281] Publishing information on Government requests and how the company responded increases awareness among users of the scale and scope of Government requests, and increases transparency about corporate responses. The first transparency report was published by Google in 2010. To date, there is not a standardised method of publishing the information, and therefore each company transparency report differs slightly, making comparison difficult, but as more companies publish reports, there has been an effort to move beyond publishing mere numbers and add context on the laws governing censorship and surveillance, including areas where companies are prevented by law from disclosing information. Providing this additional context highlights the responsibilities of the Government and areas where disclosure and transparency can be improved.
- **Report according to the US State Department Requirements for US Companies:** The State Department requires all companies investing US$500,000 or more in Myanmar to submit an annual report on their activities, covering areas including land, labour, environmental and other human rights. TPG Holdings, which through its jointly owned company Apollo Towers, is engaged in the construction and operation of telecommunications towers submitted a report in 2014.[282]
- **See also Chapter 4.4 on Surveillance.**

D. Relevant International Standards and Guidance on Freedom of Expression

Relevant International Standards:

- Universal Declaration of Human Rights (Article 19)
- International Covenant on Civil and Political Rights (Article 19)
- Freedom Online Coalition, Tallinn Agenda for Freedom Online (2014)

Relevant Guidance:

- Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, Frank La Rue, A/HRC/17/27 27th May 2011
- UN Human Rights Council, The Promotion, Protection and Enjoyment of Human Rights on the Internet, A/HRC/20/L.13 29th June 2012

investment obligations, and the form and extent of any ongoing government support. If IFC is financing the privatisation of such distribution services, IFC also encourages the public disclosure of concession fees or privatisation proceeds. Such disclosures may be made by the responsible government entity (such as the relevant regulatory authority) or by the client."

[280] Freedom Online Coalition, "Draft Report Executive Summary" Working Group 3: Privacy and Transparency (May 2015).

[281] See, Access Transparency Reporting Index, a record of transparency reports published by Internet companies and telecommunications companies.

[282] TPG Holdings, "Re: Report on Responsible Investment in Myanmar" Letter to the US Department of State (1 April 2014).

4

4.2

Chapter 4.2
Hate Speech

4
4.2

Chapter 4.2
Hate Speech

In this Chapter:

A. Context

Short Explanation of Hate Speech and the ICT Sector

The question of how to address certain forms of speech considered harmful has been the source of long-running global discussions. In particular, the rapid development of ICT platforms, such as the Internet and social media, has enabled wider and instantaneous dissemination of a wide range of content. It is inevitable that some of this content may be national/xenophobic, involve religious and racist hatred that incites discrimination, hostility and violence or even propaganda for war. While international human rights law and many national constitutions around the world provide for a presumption of freedom of expression, there are some legitimate, permitted restrictions of freedom of expression under international human rights law and standards (See Chapter 4.1 on Freedom of Expression). Some countries prioritise freedom of speech over most countervailing interests, even when the speech is filled with hatred. Under international human rights law and in many countries, hate-filled speech forfeits some or all of its free-speech protection in favour of protection for the dignity or equality of those who are attacked. Hate speech is not protected by international human rights law; it is prohibited and frequently punishable under national criminal law.

Hate Speech in Myanmar

In Myanmar, freedom of expression is a sensitive and complex issue. Long-running inter-communal tensions appear to be amplified by new-found expression on the Internet, which is finding a growing audience online. This issue has become particularly evident in

attacks against Muslims, women and LGBT people on popular social media websites.[283] The increasing anti-Muslim rhetoric has been particularly prevalent since the outbreak of inter-communal violence between Muslims and Buddhists in Rakhine State during 2012. While there are not many user-generated platforms currently operating in Myanmar, there are currently over three million users of Facebook, the most popular social media platform, and 12 million users of Viber, the most popular messaging app[284], with the market likely to dramatically expand.

The well-known activist Nay Phone Latt, himself imprisoned under the previous government and now leader of the free speech organisation Myanmar ICT Development Organisation (MIDO)[285] and the anti-"hate speech" campaign Panzagar,[286] has expressed concern that "hate speech" (see below) is damaging new-found freedom of expression in Myanmar. He is concerned that the Government will try to tackle it by creating new laws that may result in further restrictions on freedom of expression. In an April 2014 interview with Myanmar magazine *Irrawaddy* Nay Phone Latt said:

> *"I don't want to ask the government to control hate speech because if they control the hate speech, they will want to control all [opinions]. So it can harm freedom of expression. I prefer to monitor hate speech and report about that than limiting it through law."*[287]

This highlights the difficulties faced in finding the right balance between protecting those who are subject to hate speech and discouraging governments from extending restrictions to other types of speech a government might find offensive, such as criticism. The risk in opening the door to such restrictions may be particularly high in countries like Myanmar with a history of suppression of free speech. Civil society is justifiably concerned about giving up new and hard fought freedoms of expression.

What is said online does have the potential to spill over into real world violence. In July 2014, riots broke out in Mandalay following unconfirmed reports circulated online that a Buddhist woman was raped by Muslims.[288] Such reports proved to be false, but one Muslim and one Buddhist were killed during the violence. While President Thein Sein has publicly condemned the violence, and committed to take action against those who allegedly perpetrated it,[289] the authorities have not done enough to prevent and quash inter-communal violence and violence against Muslims. After the 2012 violence in Rakhine State, international human rights groups reported that the security forces stood by and did not adequately protect Muslims against Buddhist violence, nor did they sufficiently condemn such actions.[290] While some parts of Myanmar civil society are taking action to promote interfaith harmony,[291] they have received anonymous threats via SMS on their phones.

---

[283] Inter-communal violence between Buddhists and the Muslim Rohingya minority broke out in Rakhine State during 2012, killing 250 people and displacing almost 140,000 people, most of them Muslims. Al Jazeera English "Facebook in Myanmar Amplifying Hate Speech?" (14 June 2014).
[284] DVB, Viber Leads the Apps for Myanmar Activists, But Is It Safe To Share? (10 August 2015).
[285] See: http://myanmarido.org/en
[286] See: https://www.facebook.com/supportflowerspeech
[287] San Yamin Aung, The Irrawaddy *Hate Speech Pours Poison Into The Heart* (9th April 2014)
[288] Thomas Fuller, New York Times, *Mandalay's Chinese Muslims Chilled By Riots* (12th July 2014)
[289] The Republic of the Union of Myanmar, President Office, *President U Thein Sein Appreciates Communal Unity in Mandalay*, (7 July 2014)
[290] See for example, Human Rights Watch, *All You Can Do Is Pray* (April 2013) p 10 and 15; and p 83 for government response to the violence.
[291] Samantha Michaels, Irrawaddy, *In Burma, Mixed Reactions to Suu Kyi's BBC Statements* (25 Oct 2013)

What is needed is a clear and unequivocal signal from the Government and all political parties condemning incitement to violence and other forms of hate speech and the violence itself. If powerful or influential figures use public addresses, the official press and other avenues to signal the unacceptability of speech that incites violence, hostility, or discrimination by anyone in the country this can already be an important step in limiting such speech with tools already available.

It is feared that the elections could see a rise in hate speech. There are reports that the Government of Myanmar intends to work with Facebook to remove posts which can incite violence [292]. Achieving the correct balance between addressing hate speech and restricting free speech is always challenging. There have been combined efforts in other countries by governments, business and civil society to reduce the spread of inciteful speech during elections that might provide important lessons learned.[293]

Rather than making sweeping restrictions on content or seeking to block whole ICT services that carry such messages, the Government should pro-actively use the power of ICTs to counter rumours with fact and promote messages of non-violence. These signalling actions have not yet been taken and should be a pre-cursor to be tested in the country before any further, more serious steps to restrict freedom of expression are considered.

Hate Speech under International Human Rights Law

Defining 'Hate Speech'

'Hate speech' [*a-moun sagar*] is now a well-used phrase in Myanmar (and globally), but it is not a term recognised in international human rights law. *The International Covenant on Civil and Political Rights* (ICCPR)[294] sets certain restrictions on the right to freedom of expression but does not use the term 'hate speech' (see the discussion below on Articles 19 and 20 of the ICCPR). 'Hate speech' has become a vague term that often encompasses both expression that can be restricted under international law, and legitimate, even if offensive, expression that cannot. It is not always easy to distinguish where freedom of expression ends and legitimate restriction on expression begins. What is considered hate speech in one country may not be considered hate speech in another; it may be region or culture-specific, rooted in a country's history. Hate speech often reflects deep-rooted societal tensions and attitudes, but the lack of an internationally agreed definition of 'hate speech' has made it difficult to clarify how such acts should be dealt with in the real world, including in the digital realm. The term 'hate speech' is, unsurprisingly, not defined in Myanmar's legal framework.

---

[292] 'Provocative Facebook posts may be banned ahead of Myanmar elections', Burma Times, 25 August 2015

[293] The disputed 2007 Presidential election in Kenya resulted in an outbreak of post-election violence that left over 1,000 people dead and over 600,000 people displaced. Inquiries into the violence acknowledged the role of SMS messages and blogs in exploiting tensions between ethnic communities and inciting violence. In the run up to the 2013 elections, concerns of another outbreak of violence and fears over the potential of SMS to simultaneously send messages that incite violence led the major telecommunications operator and others to agree on protocols on sending political bulk SMS during the elections. See Table 30 case study and IHRB, "Corporate Responses to Hate Speech in the 2013 Kenyan Presidential Elections: Case Study: Safaricom"

[294] ICCPR, Article 19. Myanmar has not signed the ICCPR but has been consistently urged to do so and will be asked to explain its position on the Covenant at its forthcoming review in the UN Human Rights Council under the Universal Periodic Review procedure tentatively scheduled for 20 July 2015. The ICCPR provisions are based on similar provisions of the *Universal Declaration of Human Rights*.

Permitted restrictions on expression in International Human Rights Law

Freedom of expression does not only protect popular or uncontested sentiments. It also protects views that are unpopular, or may shock, offend, or disturb. This is the nature of freedom of expression: someone may express an opinion others disagree with, but they nonetheless have a right to say it, except in certain narrowly defined circumstances. When it comes to determining what speech should be restricted in order to protect the rights of others, international human rights law provides a very high threshold that must be met before the expression can be legitimately restricted[295] or even prohibited in order to protect a wide space for all kinds of expression.

The former UN Special Rapporteur on the Promotion and Protection of Freedom of Opinion and Expression, Frank La Rue, summarises this in a 2012 report:

> *"The right to freedom of expression implies that it should be possible to scrutinise, openly debate and criticise, even harshly and unreasonably, ideas, opinions, belief systems and institutions, including religious ones, as long as this does not advocate hatred that incites hostility, discrimination or violence against an individual or a group of individuals."*[296]

As such, expression that is "*any propaganda for war*" or "*advocacy of national, racial or religious hatred that constitutes incitement to discrimination, hostility or violence*…"[297] should proactively be prohibited by law according to Article 20 of the ICCPR. Incitement is also recognised as a crime in other international human rights treaties. The UN *Convention on the Prevention and Punishment of the Crime of Genocide* (1948) criminalises a "*direct and public incitement to commit genocide*."[298] The *International Convention on Elimination of All Forms of Racial Discrimination* (1966) requires states to criminalise the dissemination of ideas based on racial superiority and assisting or financing racist activities.[299] One unfortunate omission, however, concerns gender which is not specifically considered in these instruments. Nor is advocacy of hatred that incites violence towards women provided for in the *International Convention on the Elimination of all Forms of Discrimination against Women* (1976).

National Legal Framework

The 2008 Myanmar Constitution does not prohibit incitement to hatred, as is the case in many domestic legal frameworks around the world. It does have constitutional protections against discrimination: Article 348 of the 2008 Constitution guarantees that discrimination by the Union against any citizen is prohibited on the grounds of race, birth, religion, official position, status, culture, sex and wealth. However, the internationally recognised grounds

---

[295] Harmful speech can also be restricted under articles 18 and 19 of the ICCPR on the grounds respect for the rights of others, public order, or even sometimes national security if the restrictions meet the tests set out under Article 19 (see Chapter 4.1 on Freedom of Expression for an explanation of the tests).
[296] UN General Assembly, "Promotion and Protection of the Right to Freedom of Opinion and Expression. Note by the Secretary General". (10th August 2011), A/66/90, Para 30.
[297] *ICCPR*, Article 20. Hatred, by itself, would not be subject to restriction. It is only when advocacy of national, racial or religious hatred constitutes incitement to discrimination, hostility or violence that it must be restricted under international law.
[298] *UN Convention on the Prevention and Punishment of the Crime of Genocide* (1948) Article III(c).
[299] Article 4(a): *"Shall declare an offence punishable by law all dissemination of ideas based on racial superiority or hatred, incitement to racial discrimination, as well as all acts of violence or incitement to such acts against any race or group of persons of another colour or ethnic origin, and also the provision of any assistance to racist activities, including the financing thereof."*

of discrimination based on colour, language, political or other opinion and national origin are not prohibited. Moreover, Article 349 applies only to Myanmar citizens.

Several laws in Myanmar provide for broad and vague restrictions of the right to freedom of expression and peaceful assembly (see Chapter 4.1 on Freedom of Expression) that could be used to block such incitement. These are, however, problematic because they can also be used to restrict far wider types of expression. There are widespread concerns globally that governments use prohibition on incitement to prohibit much wider types of expression, using often vaguely defined national laws that opens the door for arbitrary application of these laws. [300] Sections 295(A), 298, 504, and 505 of the *Myanmar Penal Code*, covers "[a]*cts or words which intentionally cause outrage or wound religious feelings"* and "[s]*tatements or insults which intentionally provokes a breach of the peace or causes public mischief*." While these provisions have some overlap with Article 20 of the ICCPR, they cover a much wider set of issues than incitement to hatred and therefore are not sufficiently targeted to meet the legal tests set out in international human rights law to be considered legitimate restrictions of freedom of expression.[301] Phrases like "*causing public mischief*" can be used to justify suppression of politically problematic speech i.e. the type of speech that is protected under international human rights law to ensure open and vibrant democratic debate. The right to freedom of expression is intended to protect speech that may create "*outrage*" among some, to ensure governments do not become the sole arbiter of opinion and expression.

B. Field Research Findings

Methodology

In February-March 2015 IHRB/MCRB undertook qualitative research on social media in Myanmar by conducting a short monitoring survey. While by no means a comprehensive study, it aimed to provide a snapshot of the current atmosphere on social media in Myanmar to gain some contextual understanding of this relatively new issue of hate speech and provide useful observations and recommendations as part of this broader ICT SWIA. This short study drew on the authoritative work of Professor Susan Benesch of the Dangerous Speech Project.[302]

The 'Dangerous Speech' Framework

Academics have noted particular characteristics of speech that rise dramatically before an outbreak of mass violence. There have been efforts to test the direct correlation between such speech and subsequent acts, whatever the means of communication.[303] While such

[300] OHCHR, "Rabat Plan of Action on the Prohibition of Advocacy of National, Racial or Religious Hatred that Constitutes Incitement to Discrimination, Hostility or Violence" (2012), para 15. See also, OHCHR, "Concept Paper on OHCHR's Expert Workshops on the Prohibition of Incitement to National, Racial or Religious Hatred" (2011).

[301] Article 19(3) of the *ICCPR* provides any restrictions must pass a three-part, cumulative test: be provided for in national law which is clear and accessible to everyone (principle of legal certainty, predictability and transparency); have a legitimate aim or purpose i.e. one of the purposes set out in Article 19.3 (principle of legitimacy); and must be necessary and proportionate to the legitimate aim pursued, meaning that the restrictions must the least restrictive means required and justifiable (principles of necessity and proportionality).

[302] See: http://www.dangerousspeech.org/

[303] See David Yanagizawa, "Propaganda and Conflict: Theory and Evidence from the Rwandan Genocide" (2012). A statistical study shows that killings were 65-77% higher in villages that received the Radio Television

examples of speech may not necessarily fall under the restrictions set out in the ICCPR, the development of the Internet and the use of social media provide a platform that can amplify this kind of speech. Attempts are underway to predict the likelihood of certain speech catalysing real world violence in certain situations.

The Dangerous Speech Framework aims to find patterns in speech common before an outbreak of violence by identifying speech which targets members of a particular group, and which may have the potential to catalyse an outbreak of violence by encouraging people to condone or take part in violent acts. The framework's guidelines are based on five variables[304], used to assess the potential impact of a particular speech.

The most dangerous speech would be one for which all five variables are present:

- A powerful speaker with a high degree of influence over the audience;
- The audience has grievances and fear that the speaker can cultivate;
- A speech act that is clearly understood as a call to violence;
- A social or historical context that is propitious for violence, for any of a variety of reasons, including longstanding competition between groups for resources, lack of effort to solve grievances, or previous episodes of violence;
- A means of dissemination that is influential in itself, for example because it is the sole or primary source of news for the relevant audience.

Questionnaires

MCRB and IHRB developed a questionnaire based on these variables, drawing on an existing questionnaire developed by Professor Susan Benesch and the Kenyan organisation Ushahidi, which ran the Umati [305] project monitoring dangerous speech before and during the Presidential elections in Kenya in 2013.

A mother-tongue Burmese-speaking researcher helped develop the questionnaire[306] for the Myanmar context and conducted research on social media websites in Myanmar. The researcher was asked specifically to search for examples of what they believed to be 'hate speech' and apply the questions outlined in the questionnaire to them. The researcher collected 42 examples of 'hate speech' over a two month period (February and March 2015), which were then analysed.

Reporting the Results

Studying hate speech presents an ethical dilemma: re-publishing examples may perpetuate the sentiments in the message. We have taken the decision not to re-publish statements and photographs here. The presentation of results below summarises the findings.

Libre de Milles Collines (RTLM) signal. Two RTLM executives were convicted of incitement to genocide in 2007. See also Koigi Wa Wamwere, *Negative Ethnicity: From Bias To Genocide* (2003), Seven Stories Press, New York. Pp103-105, which describes anonymous leaflets circulated in Nazi Germany propagating hatred against Jews. More recently, leaflets were circulated provoking ethnic hatred during the break up of Yugoslavia, during the violent end to apartheid in South Africa instigating violence between the Xhosas and Zulus and have also been circulated in Kenya warning certain communities to leave their homes or be killed.

[304] See: http://www.dangerousspeech.org/guidelines

[305] See: http://www.ihub.co.ke/umati

[306] MCRB, IHRB, DIHR, "SWIA Questionnaires" (May 2015).

Key Observations

Human Rights Implicated: Right to freedom of expression, opinion and information; Right to privacy

- All examples on Burmese social media were **written in Burmese**, with one exception.
- 88% of examples contained language **directed primarily at the Muslim community**.
- **12% of these fitted the criteria of the most dangerous forms of speech**:
  - There were several examples of a powerful or influential speaker who capitalised on a fear of the audience, including calls to action such as violence against a community where there have been previous episodes of inter-communal violence.
  - These examples were shared widely on social media, potentially reaching millions of users.
  - However, while this could be considered an influential means of dissemination, social media is not the sole or primary source of news in Myanmar.
- **All of the samples suggested the audience faced danger from Muslims**, either a threat that Muslims are becoming too dominant in society, or that they are spoiling the integrity of Myanmar, for example by marrying Buddhist women.
- **38% of samples included a call to action**, either to discriminate (e.g. by avoiding Muslim-owned shops and businesses), hostility (e.g. that Muslims should be denied citizenship or ethnic minorities should be driven out of the country) and actual calls to kill Muslims.
- **The researcher considered 30% of samples to have fake profile names** and were therefore anonymous or not identifiable. For example, several user names were recognisable as names of characters in Burmese novels, or translated into English as phrases like "*a beautiful evening*". Some user names had more intimidating translations, for example "*the person who guards ethnicity*" or phrases intended to be insulting to Muslims.
- **Around 10% of samples compared Muslims to certain animals.** The Dangerous Speech Framework includes, as part of the variable on 'speech', referring to people as other than human (e.g. vermin, pests, insects or other animals) as an attempt to de-humanise the victim and one indicator of violence.
- **17% of samples used language or symbols specific to Myanmar**, such as images of someone or something being stepped on, considered an insult in Burmese Buddhist society, or using the style of Buddhist teaching or proverb in a derogatory way to Muslims.
- **The posts that were shared most widely** were quotes by well-known Burmese figures, links to news articles or alleged accounts of killings of Buddhists by Muslims (all unconfirmed), or calls to boycott Muslim-owned shops and businesses.
- **The posts that received the most reaction/response were those made by a politician or religious leader.** One politician alleged a Muslim had set a school on fire, which was shared 1,300 times. The same politician advocated the burning of a mosque if it was built in a particular area, and received over 1,000 positive responses. A religious leader's post encouraging people not to give housing to Muslims received 1,300 positive responses and was shared 830 times.
- **When influential figures, such as a politician or religious leader, made statements against Muslims, supporting comments by normal users were the most violent** of the samples, including calls to kill Muslims.
  - In the recorded examples, explicit calls to kill Muslims were posted as comments

in response to a religious leader's post containing allegations that a Muslim man had raped a Buddhist woman.
  - Another call to kill Muslims was a comment on a widely shared news article, believed to be fake, that a Burmese soldier had been killed by a Muslim.
- Most of the examples of posts by normal users had few followers or reactions and were not shared widely. However, **the most popular post** of all the examples in the study was **a normal user sharing the alleged restrictions the country of Japan places on Muslims entering and living in the country**, which is untrue**.** This was shared over 18,000 times.
- Even where the user was not a well-known figure, **content relating to current events in Myanmar received the most reaction,** such as the Presidential revocation of 'white cards',[307] a temporary identification card, from displaced and stateless Muslims applying for citizenship, or advising women to be wary of Muslims during Thingyan (the Buddhist Water Festival in April).

Conclusion of Field Research Observations

The observation provoking the most serious concern from this short monitoring study is the impact of people in positions of influence, such as politicians or religious leaders, making statements that may incite violence, hatred, or discrimination. These public statements appear to encourage other users to repeat the sentiments, and even go further, such as issuing calls to kill people. This is particularly worrying as Myanmar approaches elections, because they have the potential to incite violence.

C. Hate Speech: Recommendations for ICT Companies

- **Identify the potential impacts a company may have**: For example, decisions taken by ICT companies on how to tackle hate speech have the potential to impact the right to freedom of expression by:
  - Providing access to platforms that allow user-generated hate speech content to flourish;
  - Making their own internal decisions to remove content
  - Responding to government requests to block access to certain websites or remove particular content that may be hate speech or may be other types of permitted speech that the government has chosen to label as hate speech.
- **Understand the legal framework:** As outlined above and in Chapter 4.1 on Freedom of Expression, the legal framework that could be applied to online communications contains vague and undefined terms. While these vague terms could be used to block access to national, racial or religious hatred in line with Article 20 of the ICCPR, those same provisions are so broadly worded that they could result in legitimate content being removed or blocked as well. The Government or other groups' (such as religious or ethnic groups) may request or require that companies restrict freedom of expression that does not fall within the permitted restrictions under Article 19 or the prohibitions under Article 20. In such cases, an ICT company will find it challenging to

[307] Radio Free Asia, Myanmat Authorities Step Up Collection of Temporary Identification Cards (6 April 2015).

meet its responsibility to respect human rights under the UN Guiding Principles, and may finding itself potentially contributing to government or non-state actors' abuses of individuals' human rights. Likewise, because the government does not have precise laws prohibiting hate speech, ICT companies may permit the transmission or hosting of expressions that would be considered incitement to national, racial or religious hatred.

- **Understand the local context:** It is important that ICT companies understand the context in which they are working and have processes in place to deal with Government and others' attempts to restrict freedom of expression. They need to be able to assess whether the requests are legitimate and do not amount to censorship and to understand what may be hate speech and therefore appropriately prohibited or deleted on platforms or services. Moreover, many services that can be accessed in Myanmar are provided by international companies which are not based in the country, and they may not even have offices or staff on the ground. They may therefore not have experience of the country or be aware of cultural and political sensitivities or have the appropriate language capabilities to screen content posted on their site. Additional measures will need to be taken to ensure a realistic and systematic understanding of the local context, such as obtaining independent expert advice. (See Chapter 4.1 on Freedom of Expression).

Different players in the ICT value chain will have different responsibilities:

Operators/Telcos/Internet Service Providers (ISPs)

- **Put in place processes to deal with Government requests**: Companies that provide Internet access may be asked by the Government to block access to whole websites due to the perceived spread of hate speech.[308] This reportedly happened in Myanmar during the riots in Mandalay in 2014. A high-ranking police officer said in an interview that the government had ordered the blocking of a popular social media website to stop the spread of "*unverified news*", which coincided with a curfew imposed on Mandalay residents.[309] The reason for blocking the website was to prevent the spread of further rumours fuelling violence. However, as noted above, because Myanmar laws are often vague and not aligned with international human rights law, such requests may also cover legitimate expression that should not be blocked or taken down. It is currently unclear how requests for blocking websites are made to ISPs in Myanmar, either by law enforcement agencies directly or a request made through the regulator. It is also unclear under what circumstances requests to block whole websites can be made as there is little legislation covering this area and therefore ISPs appear to be voluntarily blocking websites. In other countries, the most common reason for blocking websites is related to child exploitation, terrorism or copyright infringement.
- **Develop clear processes for blocking websites**: In the example of the Government request above, the order to block this particular website would have been made to the operator or ISP providing Internet access. Blocking whole websites may prevent

[308] Facebook's Government Requests Report noted that in the period July-December 2014, the company "restricted access to 5 pieces of content reported by the President's Office based on sections 295(A), 298, 504, and 505 of the *Myanmar Penal Code*, which covers "*Acts or words which intentionally cause outrage or wound religious feelings"* and "*Statements or insults which intentionally provokes a breach of the peace or causes public mischief*." https://govtrequests.facebook.com/country/Myanmar/2014-H2/

[309] Global Voices "Blocking Facebook: A Hot New Trend in Southeast Asia?" (11 July 2014). Original article in Burmese at http://burma.irrawaddy.org/interview/2014/07/04/61420.html.

certain people from spreading rumours, but it also prevents everyone else from seeking, receiving and imparting information and prevents authorities using it to disseminate factual information, counter rumours and appeal for calm. This may set a worrying precedent for blocking websites in the future that the government simply does not like. It is important that processes are put in place that make clear under what circumstances websites can be blocked, and how a request is made to an ISP. Requests to block from the Government of Myanmar should be made in writing; be accompanied by a court order/judicial authorisation that sets out the legal justification for the request and be time-bound.ISPs must check that requests are made in accordance with the law, and have the opportunity to clarify or request further information if needed.

'Over the Top' Services

- **Put in place processes to deal with requests from Government and users**: It is unlikely that an over the top company, such as social media sites, search engines, and blogging platforms, will be notified of or involved in a decision by the Government to cut off access to their whole service, as in the case of ISPs. They are more likely to receive requests from governments or users to remove particular pieces of offending content. Companies usually take the decision to remove content based on their own Community Standards or Terms and Conditions, which often set out what can and cannot be said on their platforms. Freedom of expression may be adversely impacted if the company's standards are not aligned with international human rights law and/or it does not properly assess the human rights impacts of the takedown request from the government or users. An example is removing content that merely expresses ideas and opinions the Government or others object to but that does not fall into a category of speech that can legitimately be restricted. However, content that falls into the category of incitement can, and should be, blocked.
- **Make Terms of Service accessible**: As most over the top companies set their own policies about which content can and cannot be posted, it is important that these Terms of Service are aligned with international human rights standards. Users then need to be aware what content is permissible on certain online services. 'Hate speech' is a relatively new concept in Myanmar and what users consider to be hate speech may differ from person to person. For example, during field research on the ground in Myanmar, some people considered swear words or general insults to be hate speech. It is important that a company's terms of service are translated into Burmese and ideally other ethnic languages, none of which are formally covered by major social media platforms. However users may use either non-Myanmar languages or transliterated forms of Myanmar ethnic minority languages. The company therefore risks hosting hate speech in any of those languages. This is an area where companies need to build up their capability to be able to screen and manage content in all languages on their sites.
- **Develop and promote reporting mechanisms:** Most online platforms have a mechanism for users to report content that is illegal, or falls under categories that the company would remove as it contravenes their terms of service, such as a user receiving abuse. As social media companies do not actively monitor all the content posted on their platform, the reporting process is important. It is unlikely the company would see this content otherwise. It also helps the company 'take the temperature' of societal attitudes and understand the context in which they are working. One of the ways in which the spread and impact of hate speech can be reduced is through a well-functioning mechanism of reporting such speech to the company hosting it, followed by a swift process of removing it from the site. This depends on (as noted above),

terms of service that are aligned with international human rights standards (given that the government currently does not have clear laws or guidance on this issue) and a transparent and accessible process for users to report content they consider hate speech. One company has developed a 'market specific' reporting mechanism unique to the Myanmar context, with an option to report specific kinds of content. One option is to report content that is, ***"****hateful towards a race, religion, gender, sexual orientation or ability. Examples: racism, insulting religious groups, anti-gay posts".* Another is to report content which is, *"a rumour or false information. Examples: false news stories, rumour based on the conflict of religious groups".*

- **Promote awareness of Terms of Service and reporting mechanisms.** Overall there is a low level of awareness of the impact of hate speech in Myanmar, and what may or may not be acceptable to post online. Many users in Myanmar are unaware of reporting functions, or do not know how to use them, or understand what action the company may take if they do report content. Companies could consider initiating a public awareness campaign focused on platform-specific guidelines and the impacts of hate speech spread through media. Materials need to be translated into local languages. Facebook Community Standards are now available in Burmese.
- **Develop other options to respond to hate speech:** Efforts are underway by civil society to educate users and combat hate speech in society. Telcos and over the top companies appear aware of the issue of hate speech in Myanmar, and some are supporting local groups to spread messages of non-violence. For example, Panzagar aims to promote responsible use of social media, and raise awareness of the implications resulting from online behavior. Panzagar has partnered with local graphic designers and Facebook to create a set of online 'stickers' with cartoons and peaceful messages, similar to emoticons, which can be downloaded and inserted onto user profiles, or included in online chat functions.[310]

D. Relevant International Standards and Guidance on Hate Speech

Relevant International Standards:

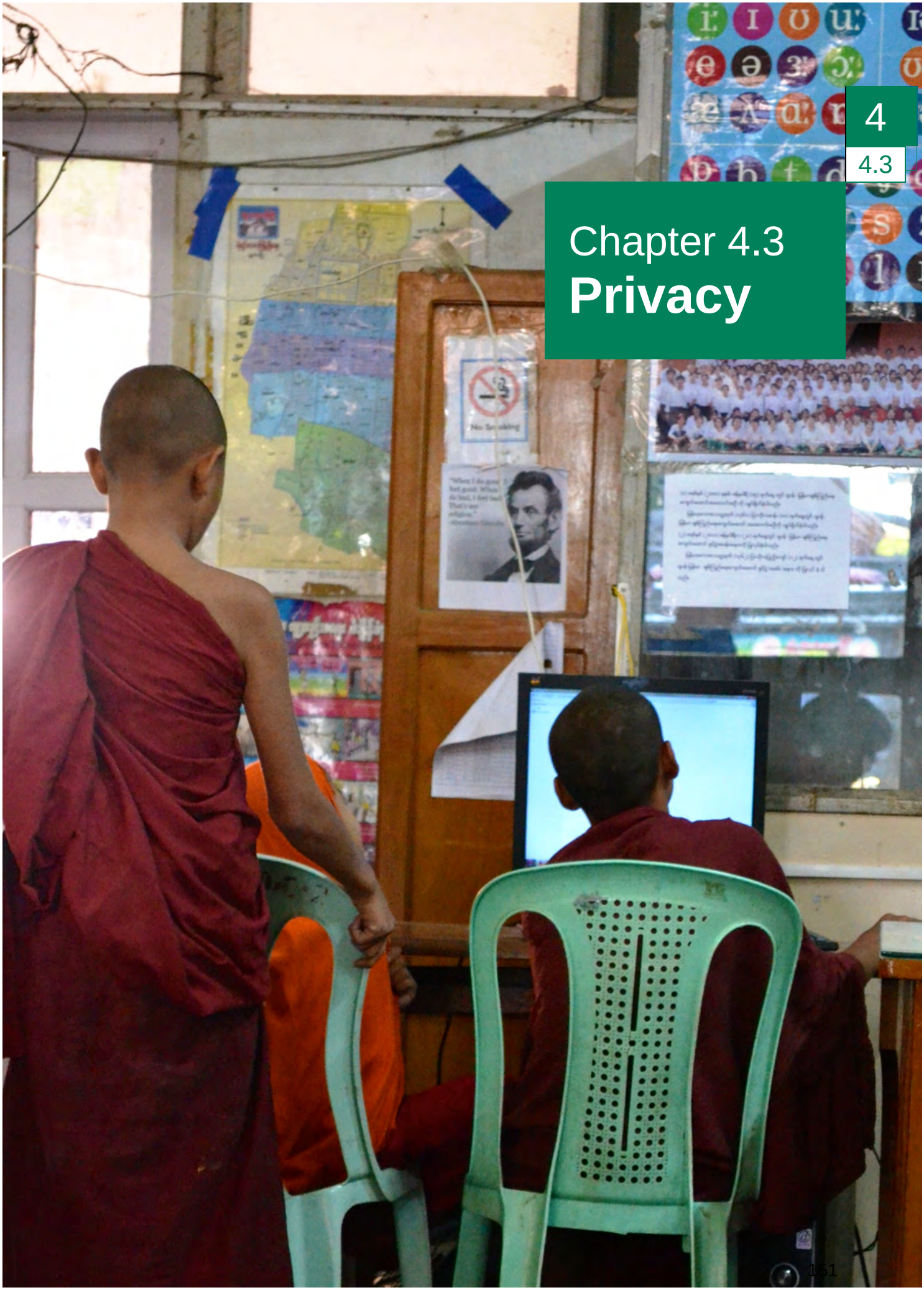
- UN OHCHR, "Report of the Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression" A/67/357 (7h September 2012).
- OHCHR "Rabat Plan of Action on the Prohibition of Advocacy of National, Racial or Religious Hatred that Constitutes Incitement to Discrimination, Hostility or Violence" (2012).

Relevant Guidance:

- ARTICLE 19, "Towards an interpretation of Article 20 of the ICCPR: Thresholds for the prohibition of incitement to hatred (Work in Progress)". A study prepared for the regional expert meeting on article 20, Organised by the Office of the High Commissioner for Human Rights, Vienna, February 8-9, 2010.
- The Dangerous Speech Project
- United States Institute of Peace, Wielding Technology to Combat Dangerous Speech in Myanmar – PeaceTech Exchange Myanmar
- NipeUkweli – This is an initiative based in Kenya to counter negative online content by correcting false statements and spreading positive messages.

[310] Global Voices, "Can #Panzagar 'Flower Speech' Facebook Stickers End Hate Speech in Myanmar?" (22 Feb 2015).

Chapter 4.3
Privacy



4
4.3

Chapter 4.3
Privacy

In this Chapter:

A. Context

Data Privacy and Data Protection

There are three dimensions to the right to privacy that are implicated by the collection, storage, use and access to digital information by ICT companies:

- data privacy or protection (the term used may differ from country to country[311]) of data held by businesses (covered in this Chapter 4.3 on **Privacy**),
- surveillance, including lawful interception and access to communications data (see Chapter 4.4 on **Surveillance**), and
- the protection of such data against attacks or threats of attack for criminal or other harmful purposes (see Chapter 4.5 on **Cybersecurity**).

In today's digital economy, the amount and type of personal information generated and stored electronically is unprecedented, ranging from email addresses, to bank account numbers, to national ID numbers. Whenever users interact with technology, such as mobile services or the Internet, 'communications data' (as it is commonly referred to in Europe), or 'metadata' (as it is commonly referred to in the U.S) is created and is typically stored by the service provider.[312] This type of data is created by a wide range of interactions with Internet services including email, web browsing, social media, search

[311] See: Baker Hostetler, "2015 International Compendium on Data Privacy Laws" (2015) and Norton Rose Fulbright "2014 Global Data Privacy Directory" (2014). Also see Francoise Gilbert "Privacy vs. Data Protection: What Is The Difference?" (1 October 2014).

[312] The National Information Standards Organization (NISO) defines metadata as "*structured information that describes, explains, locates, or otherwise makes it easier to retrieve, use, or manage an information resource.*" NISO, "Understanding Metadata" (2004), pg. 16. The former UN Special Rapporteur on Freedom of Opinion and Expression expressed particular concern over the increasing amount of metadata generated by ICT usage and its implication for user privacy. See OHCHR, "Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, Frank La Rue" A/HRC/23/40 (17 April 2013).

engines, VoIP (e.g. Skype) and mobile phones. Globally, ICT companies use this information in various ways. For example, free applications or services frequently offer the advertisers who support them a platform for user-targeted advertisements, based on data collected from users. Geographic location data can be used to identify where a user is physically located and provide location based advertisements or services such as taxis, restaurant recommendations, or directions.

As a country's ICT sector grows, more and more personal data is collected and stored by governments and companies providing goods and services online. This more extensive and innovative use of personal data brings greater economic and social benefits, but also increases privacy risks.[313] How the information is shared and who has access to it determines whether or not privacy is protected and respected.

In many countries, national data protection laws require companies to secure and protect such information from access by unauthorised third parties. Data protection or data privacy laws[314] should safeguard user privacy. Such protections are intended to regulate how, when, and why a user's personal information or data may be used or stored by a third party.

They should put limits on governments and companies concerning the collection, storage and sharing of personal data generated by using ICTs when trading, or using goods and services online. This should ensure that it is gathered for a legitimate purpose and protected from misuse. There should be restrictions or limits in each country's data protection or data privacy legislation as to how this information is collected, stored and shared by companies for commercial reasons, or by governments obtaining this kind of information for services such as voting registration, health records or tax purposes.

Legislation that regulates data privacy typically details a consent mechanism to inform and request permission from users, provides a legal definition of what constitutes personal data, mandates an allowable timeframe for the use of any data after consent is given, and includes regulatory mechanisms for pursuing grievances about the use of data. However many national frameworks lack 'use limitations', instead allowing the collection of data for one legitimate aim, but subsequent use for others.[315] In addition, a lack of a data protection framework means there is no opportunity for individuals to seek redress or compensation in cases of unauthorised sharing or use of personal data.[316] Myanmar currently lacks a data protection law.

[313] OECD, "The OECD Privacy Framework", (2013).
[314] Outside Europe, the term 'data protection' and 'data privacy' is used to commonly mean the same thing.
[315] OHCHR, "The right to privacy in the digital age", A/HRC/27/37, (June 2014), para. 27.
[316] Privacy International, "UN Universal Periodic Review, Stakeholder Report 23rd Session, Myanmar, The Right To Privacy In Myanmar", (March 2015), para 32.

4
4.3

Concerns about Privacy and Data Protection in the ICT Sector

The increasing availability of Internet services accessed via a personal computer (PC), laptop, mobile phone or other devices, has brought many benefits and is seen as crucial to continued innovation and development. But it has given rise to numerous privacy concerns about the data that is collected, stored and shared when using such services. The collection and use or misuse of sensitive data has the potential to be used for discriminatory purposes. This could include data on racial origin, political opinions or religious or other beliefs, personal data concerning health or sexual life, genetic data, biometric information, trade-union membership, and data relating to criminal convictions. Unauthorised intrusions to access or destroy data stored for use in criminal purposes – such as unauthorised access to bank accounts – is an issue rising rapidly up the list of key concerns for many businesses. New business models based on the collection and sale of a user's data by the company gathering the data, where data is used for purposes not explicitly revealed to the user who provided the data and without their permission, raise concerns about the respect for user privacy.[317]

While 'Big Data'[318] may carry important benefits, it also carries serious risks. Data mining of large data sets has the potential to be discriminatory. It may discriminate against specific groups and activities (such as in profiling) and it may be used to draw conclusions about large groups of people who may be excluded from data collection, further perpetuating exclusion.[319] In addition to more generalised areas of data protection, there are other areas of online protection that have generated real concern, particularly around the protection of children who are active online.

Table 38: Toward a Social Compact for Digital Privacy and Security[320]

Below are excerpts of the core elements that the Global Commission on Internet Governance advocates in building a new 'social compact' for digital privacy and security:

- "*Fundamental human rights, including privacy and personal data protection, must be protected online. Threats to these core human rights should be addressed by governments and other stakeholders acting both within their own jurisdiction and in cooperation.*
- *Businesses or other organisations that transmit and store data using the Internet must assume greater responsibility to safeguard that data from illegal intrusion, damage or destruction. Users of paid or so-called 'free services' provided on the Internet should know about, and have some choice over, the full range of commercial*

[317] The Global Commission on Internet Governance was established in January 2014, to articulate and advance a strategic vision for the future of Internet governance. With work commencing in May 2014, the two-year project will conduct and support independent research on Internet-related dimensions of global public policy, culminating in an official commission report.
[318] 'Big Data' refers to large datasets that are collected and analysed to find correlations or predict trends. For example, it can be used by business to predict which products will be popular, but can also be used for social issues, such as predicting outbreaks of disease in certain areas.
[319] See Privacy International, "Data Protection" (last accessed August 2015). See also, European Commission, "EU Data Protection Reform and Big Data, Factsheet" (April 2015).
[320] Global Commission on Internet Governance, "Toward a Social Compact for Digital Privacy and Security Statement" (2015).

use on how their data will be deployed, without being excluded from the use of software or services customary for participation in the information age. Such businesses should also demonstrate accountability and provide redress in the case of a security breach.

- *There is a need to reverse the erosion of trust in the Internet brought about by the non-transparent market in collecting, centralising, integrating and analysing enormous quantities of private information about individuals and enterprises — a kind of private surveillance in the service of 'big data', often under the guise of offering a free service."*

Increasingly, there are calls for standards and accountability mechanisms to bolster confidence in the use of the Internet. 'Data due process', access to remedy, and greater transparency – by governments and business – are all being advocated as important steps in maintaining an open and accessible Internet.

In addition, because companies may hold a lot of personal information, they may be subject to requests to hand over information about a user to a government - with or without legal authorisation - in a manner that is not in line with human rights. When a country's law enforcement or intelligence agencies request, access or intercept information collected and stored by ICT companies to support law enforcement or national security investigations, this triggers privacy concerns. This dimension is addressed in Chapter 4.4 on Surveillance.

Privacy in the Myanmar Context

In Myanmar, businesses and Government are transitioning from storing information in filing cabinets to electronic databases. Data can now be stored on remotely located servers, and accessed over the Internet, otherwise known as 'the Cloud'.[321] It means that users have access to an almost unlimited amount of storage of their data, which can be accessed from any computer. Cloud storage is most commonly used for email (such as Gmail) and storing data (such as Dropbox).

The improved efficiency and ease of access provided by digitally storing information is obvious, as are the potential human and commercial risks and need for accompanying legal frameworks. Myanmar companies who long operated in isolation may be finding that data protection requirements are now necessary if they are involved in the cross-border exchange of commerce and data. ASEAN has already put in place frameworks on data protection, as have other regional bodies,[322] including the EU, where appropriate data protection is a prerequisite of before any data can be transferred from the EU.[323]

[321] In the simplest terms, cloud computing means accessing files and applications over the internet, rather than on personal hard drives or servers, via third party services.
[322] See in particular, the basic principles on data protection in the OECD, "Guidelines Governing The Protection Of Privacy And Transborder Flows Of Personal Data" (2013).
[323] Under the EU Data Protection Directive, personal data may only be transferred to third countries i.e. countries outside of the European Union, if that country provides an adequate level of data protection. This created an incentive for some countries to increase data protection standards, due to the economic benefits through increased trade with EU countries.

Equally, whereas protection of privacy was until recently an unknown concept in Myanmar, awareness is growing among the Myanmar business community about the importance of personal data protection even without mandated privacy standards, such as for emerging services such as mobile money.[324] As users weigh competing services, companies that fail to provide strong data safeguards may start to find they lose customers, although currently, the public's awareness of the need to protect personal data is quite low. A recent high profile case involving a (now dismissed) employee of an operator giving unauthorised access to communications data to a friend will have further served to raise awareness[325].

In May 2013, Human Rights Watch sent a letter to mobile network operators shortlisted in the MCIT telecommunications license process seeking clarification regarding how new telecommunications firms entering Myanmar would seek to mitigate potential human rights impacts given Myanmar's lack of legislation related to privacy, censorship, and interception. Both Telenor and Ooredoo issued responses. Their company positions on data privacy took different approaches. MPT and Yatanarpon Teleport have not issued public statements on data privacy. Myanmar's remaining Internet service providers also do not provide any clarification on data privacy policies on their websites.

Ooredoo highlighted its "*commitment to Myanmar to use Singapore as a benchmark"* and the intent to "*implement policies and procedures that are compliant with the 2012 Singapore Data Protection Act.*"[326] The Singapore *Data Protection Act* (PDPA) defines personal data as "*data, whether true or not, about an individual who can be identified from that data; or from that data and other information to which the organisation has or is likely to have access.*" [327] The PDPA requires private sector companies to notify and provide individuals with an explanation when their personal data is collected and disclosed. With regard to telecommunications, the Singapore Personal Data Protection Commission has issued advisory guidelines for the telecommunications sector.

However, the Singapore PDPA does not provide adequate protection for human rights. It lacks references to specific and relevant human rights principles under international law, exempts Government agencies and entities working on their behalf, has ambiguous limitations on legitimate purpose for data collection and disclosure under the PDPA, exceptions to individual consent requirements, poor transparency and accountability mechanisms, and broad language that allows for organisations and data to be exempt from PDPA regulations in the future.[328]

Telenor's response to Human Rights Watch's letter cited Telenor's "*well established privacy and data protection regime*".[329] A section of the Telenor website explains that, "*Telenor Group only processes personal data for the purposes the data was originally*

[324] See Myanmar Times, "Preparing the Financial System for Digital Attacks" (March 2015)
[325] 'Ooredoo data breach brings legal action', 3 September 2015, Myanmar Times.
[326] Ooredoo response to Business and Human Rights Resource Centre's request for a response to HRW's Report: Burma Telecom Winners Should Safeguard Users
[327] Personal Data Protection Commission Singapore, "Legislation and Guidelines: Overview" (last accessed August 2015).
[328] Internal analysis prepared for the Institute of Human Rights and Business.
[329] Human Rights Watch, "Response from Ms. Oldgard, Vice President, Head of Group Corporate Responsibility, Telenor Group" (4 June 2013).

collected, and only for as long as the purpose exists. The companies in Telenor Group will ensure that:

- "Persons we process data about are properly informed when their personal data is being collected;
- All persons we process information about have the right to obtain relevant information on the processing of personal data related to them;
- Persons we process and store data about are able to exercise user choice and control and have appropriate rights to correct or delete their personal data;
- Personal data are kept in a form which permits identification of persons for no longer than is necessary for the purposes for which the data were collected;
- Transfer of personal data does not compromise an adequate level of protection;
- Risk based, planned and systematic measures are undertaken to ensure satisfactory information security in connection with the processing of personal data;
- The processing of personal data is properly documented;
- Appropriate training is given to relevant personnel involved in the processing of personal data."[330]

Telenor specifically cited its participation in privacy projects with the GSMA (where it is a full member),[331] and the European Telecommunications Network Operator's Association (ETNO) working group on data protection[332]. In their Mobile Privacy Principles, the global industry association GSMA defines personal data more specifically than Singapore does in the PDPA. While acknowledging that personal information ultimately depends on its local legal definition, the GSMA defines personal data as:[333]

- "Any data that is collected directly from a user (e.g. entered by the user via an application's user interface and which may include name and address, credit card details);
- Any data about a user that is gathered indirectly (e.g. mobile phone number, email address, name, gender, birth data, location data, IP address, IMEI, unique phone ID);
- Any data about a user's behavior (e.g. location data, service and product use data, website visits);
- Any user-generated data held on a user's device (call logs, messages, user-generated images, contact lists or address books, notes, and security credentials."

The ETNO works closely with the GSMA, and focuses on the review of legal frameworks impacting data protection in Europe. In terms of data protection and privacy, the draft EU General Data Protection Regulation (GPDR) is regarded as providing high standards in the protection of personal data by the international community.[334] As part of that process, the ETNO has supported the notion that there should be no preferential treatment in data

[330] Telenor Group, "Our Privacy Position" (last accessed August 2015).
[331] GSMA, "Mobile and Privacy" (last accessed August 2015). The GSMA is an industry association representing mobile operators worldwide.
[332] ETNO, "Data Protection, Trust & Security" (last accessed August 2015).
[333] GSMA, "Mobile Privacy Principles" (2012).
[334] See European Commission, "Proposal for a Regulation Of The European Parliament And Of The Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation)" (25 January 2012). The legislation is not without criticism from global technology firms such as Google who have recently complied with users' "right to be forgotten and to erasure" requests under Article 17 of the GPDR. Telenor Myanmar is a wholly owned subsidiary of the Telenor Group per the license requirements stipulated by MCIT. Telenor Group is headquartered in Oslo, Norway. Norway is not a member state of the European Union but has implemented the EU Data Protection Directive 95/46/EC.

protection requirements between the private and public sectors.[335] This is a notable difference between the GPDR and the PDPA in Singapore.

As the UK NGO Privacy International notes in their submission to Myanmar's Universal Periodic Review (UPR) at the Human Rights Council, whilst some ICT companies, such as Telenor, have developed and adopted their own data protection and retention policies, the lack of national legislation regulating data retention and the circumstances under which the Government can request access to user data means that such internal policies may not be strong enough to protect the privacy of users and secure the freedom of services.[336]

In recent years, many other countries have passed data protection or data privacy legislation for the first time or updating them in response to the impact of ICTs on privacy.[337] In Asia, in addition to Singapore, Malaysia, and Taiwan have a "*Personal Data Protection Act*".[338] The law of Japan is called "*Act on the Protection of Personal Information*".[339] South Korea's law is called the "*Protection of Personal Data Act*".[340] The equivalent law of the Philippines is called the "*Data Privacy Act*".[341]

International Human Rights Law on Privacy

Every person has the right to privacy under international human rights law, including privacy of his/her communications.[342] Article 17 of the *International Covenant on Civil and Political Rights* (ICCPR) provides:

> *"1. No one shall be subjected to arbitrary or unlawful interference with his privacy, family, home or correspondence, nor to unlawful attacks on his honour and reputation.*

---

[335] ETNO, "ETNO supports the choice of the legal instrument for the future Data Protection framework" (4 July 2014).
[336] Privacy International, "UN Universal Periodic Review, Stakeholder Report 23rd Session, Myanmar, The Right To Privacy In Myanmar" (March 2015), para 33. See also A Alderaro, "Digitalizing Myanmar: Connectivity Developments in Political Transition", *Internet Policy Observatory*, (2014) pg. 10.
[337] In the European Union, the suite of laws protecting personal data are currently being updatedIn 2012, the European Commission proposed to unify data protection in the EU under a single law, the General Data Protection Regulation (GDPR), to take into account technological developments such as social networking and cloud computing. A draft was presented at the European Parliament in March 2014. A final version is expected to be adopted by end 2015. See: Greens/EFA "EU General Data Protection Regulation State of play and 10 main issues by Jan Philipp Albrecht" (17 January 2015) and European Commission, "Commissioner Jourová: Concluding the EU Data Protection Reform is essential" (28 January 2015).
[338] See Malaysia and Taiwan *Personal Data Protection Acts*.
[339] Government of Japan, *Act on the Protection of Personal Information Act No. 57* (2003)
[340] Korean LII, "Personal Information Protection Act" (last accessed August 2015). See also Francoise Gilbert, "Privacy v. Data Protection. What Is The Difference?" (1 October 2014).
[341] Republic of the Philippines *Act No. 10173 2012 Data Privacy Act*.
[342] The right to privacy is also include in a wide range of international and regional human rights instruments, signalling its wide acceptance: Article 14 of the United Nations Convention on Migrant Workers; Article 16 of the UN Convention on the Rights of the Child; Article 10 of the African Charter on the Rights and Welfare of the Child; Article 4 of the African Union Principles on Freedom of Expression (the right of access to information); Article 11 of the American Convention on Human Rights; Article 5 of the American Declaration of the Rights and Duties of Man, Articles 16 and 21 of the Arab Charter on Human Rights; Article 21 of the ASEAN Human Rights Declaration; and Article 8 of the European Convention on Human Rights. See a compilation of privacy references in international and regional human rights instruments and see also http://gilc.org/privacy/survey/intro.html

2. Everyone has the right to the protection of the law against such interference or attacks."

Legitimate Restrictions on the Right to Privacy

Article 17 of the ICCPR on privacy is less specific about permissible reasons for restricting the right to privacy as compared to Article 19 on the freedom of expression (See Chapter 4.1 on the Freedom of Expression). Restrictions on the right to privacy must be neither "unlawful" nor "arbitrary".

A restriction is "unlawful" when the interference is not authorised by States on the basis of national law authorising interference. The national law must be sufficiently accessible, clear and precise and also must not conflict with other provisions of the ICCPR, such as the prohibition on discrimination, or the country's own constitution.

The protection against "arbitrary interference" means that the interference should be reasonable in the particular circumstances. It must be in proportion to the aim, and the least intrusive option available to accomplish the aim, and be necessary in the circumstances for reaching a legitimate aim.[343]

The Myanmar Legal Framework and its Current Application

The 2008 Constitution

Most countries have provisions to protect privacy as part of their constitution. At a minimum, these provisions usually include the rights of privacy in the home and of communications. The 2008 Constitution of Myanmar provides certain privacy protection:

"357. The Union shall protect the privacy and security of home, property, correspondence and other communications of citizens under the law subject to the provisions of this Constitution."[344]

The constitutional provisions provide for a wide scope of protection by using the term "*other communications*" but the protections are available to citizens only and are not specific about the kinds of protections it will offer. Moreover, the guarantees are "*subject to the provisions of this Constitution*" (Art. 357), which has numerous restrictions on these constitutional guarantees that are quite broad. There has been little constitutional jurisprudence developed in Myanmar, meaning there is little to rely on that might limit the application of these broadly worded restrictions.

[343] The limitation must also be shown to have some chance of achieving that goal while at the same time not being so overly restrictive that the restriction makes the exercise of the right meaningless. The onus is on the authorities seeking to limit the right to show that the limitation is connected to a legitimate aim. Where the limitation does not meet these criteria, the limitation would be unlawful and/or the interference with the right to privacy would be arbitrary. Pillay report

[344] *Constitution of Myanmar* (2008).

4
4.3

Current Legal Framework and Gaps

Although the Constitution declares that privacy will be protected under the law, currently there are no separate privacy laws in Myanmar. In addition, there is no legal framework on data protection or data privacy. A Consumer Protection Law was adopted in March 2014 but its focus is on food safety[345]. As part of its ASEAN membership, Myanmar has agreed to develop best practices on data protection by 2015 but there have been no announcements to date on forthcoming plans.[346] Civil society have highlighted that Myanmar has an opportunity to leapfrog its peers in regulating privacy, data protection, Internet governance, freedom of speech/expression (partially due to the lack of legacy regulations) and to ensure that the push to improve access does not compromise these other issues. A civil society coalition suggested a proactive discussion among Government and civil society and operators, rather than waiting until the Government demands 'private' data (for purposes of national security).[347]

The integrity of technical processes for protecting user data in Myanmar is unclear, particularly in regards to Myanmar's National Certificate Authority. Certificates have significant impacts on user privacy, as they are used to verify a chain of trust whenever a user submits personal information (such as an account username and password) to an online service. These certificates are used to verify the website's validity and prevent users from submitting data to an unauthorised third party. Myanmar's certificate authority was established under the *Electronic Transaction Law* (No.5/2004).[348] Policies and practices related to Myanmar's existing certificate authority are unclear. Websites for Myanmar's Root Certification Authority, and Yatanarpon Certificate Authority are currently offline. As the Internet now represents a global community, a lack of clear processes and transparency among certificate authorities puts users' private information at risk and promotes distrust. Recently, Google and Mozilla took steps to de-trust all certificates signed by China's National Certificate Authority.[349]

Privacy International also noted in the UPR submission,

> *"In 2013, the government announced that it would replace the paper National Registration card with a smarter digital identification card to include biometric data. Whilst it seems plans have been put on hold for such a change because of financial constraints, it is an issue that must be closely monitored as if digitised the data stored will have privacy implications which will need to be considered to ensure that the right to privacy of citizens and their personal data are protected."*[350]

---

[345] 'Burma President approves consumer protection law' Irrawaddy, 17 March 2014
[346] ZicoLaw, "ASEAN Insights, Personal Data Protection" Issue 4 (7 November 2013).
[347] Verena Weber "Diversifying the global content and apps market" (last accessed August 2015).
[348] *Myanmar Electronic Transactions Law* (2004).
[349] In April 2015, both Google and Firefox stopped trusting certificates issued by China Internet Network Information Center (CNNIC). Google noted that CNNIC had signed fake certificates for Google domains, while Firefox noted that CNNIC lacked documented PKI practices. For additional information please see: Emil Protalinski, VentureBeat "Google and Mozilla decide to ban Chinese certificate authority CNNIC from Chrome and Firefox" (April 2nd 2015)
[350] Privacy International, "UN Universal Periodic Review, Stakeholder Report 23rd Session, Myanmar, The Right To Privacy In Myanmar" (2015), para 33.

In 2014, the Myanmar Government held a public consultation on the issue of mandatory registration of personal information of SIM card and mobile phone purchasers' cards.[351] This indicates the Government may not be considering the data privacy implications of its telecommunications regulations. The mandatory registration of SIM cards in other jurisdictions has shown that there are a range of unintended consequences, prompting other governments to consider and then reject the idea.[352] MCIT proposed that mandatory SIM registration would enable new and innovative services (e.g., mobile money and mHealth services). However, where such sensitive data is exchanged, these services should be required to register for extra mobile-enabled services; such registration should always be service focused. Mandatory registration could act as a barrier to accessing mobile services because people may not have an address or registration number or may be reluctant to provide personal details due to distrust of the Government.

MCIT is yet to define its procedures for the lawful interception of user communications, or access to communications data (See Chapter 4.4 on Surveillance), though it has committed to doing so. This is a crucial and important procedure that requires further consultation and consideration before any mass collection of customer data through mandatory registration is considered. Without data retention requirements, large amount of data, held for an indefinite amount of time, would be susceptible to unlawful uses, including unauthorised surveillance, leaks, and security breaches resulting in negative, and in some cases, severe impacts on the enjoyment of the right to privacy.

B. Field Research Findings

Privacy Policies by Myanmar Companies

Human Rights Implicated: Right to privacy

Field Assessment Findings

- **MCRB reviewed the websites of 73 companies** as part of the Transparency in Myanmar Enterprises project (TiME) (or 'Pwint Thit Sa' in Burmese) to collect a small sample of the use and disclosure of privacy policies and protections by Myanmar companies.[353]
- Of the 73 company websites reviewed, **only 6 explicitly explaine how they handled and used** customers', users', workers' and others' data.
- **Only 1 company actually adopted a formal privacy policy** outlining in detail its security and data handling measures**.**
- **4 company's statements were contained within other operational policies,** such as a code of conduct or code of ethics**.**
- **1 ISP explicitly did not commit to any level of data protection**, instead confirming that it may monitor its service from time to time and disclose any information regarding customers or their use as required under national law, regulations, Government requests, or that it saw fit.
- **A majority of the companies reviewed presented no accessible information** about the ways in which they handle and use data.

[351] See: MCRB, "MCRB calls for Further Consideration of the Impacts of Requiring SIM Card Registration in Myanmar" (21 May 2014).
[352] Ibid.
[353] MCRB, "Pwint Thit Sa Project (TiME)" (2015).

- One company confirmed that it would **"*only*" guarantee the privacy of the company email system to the extent required by law**, whereas a separate statement in its Communications Policy stated that as a leading institution in Myanmar it would strive to be as open and transparent as possible while protecting privacy and personal information.

Stakeholder Engagement and Grievance Mechanisms

Human Rights Implicated: Right to privacy

Field Assessment Findings

- **The concept of privacy:** The concept of privacy as outlined in international human rights standards is not fully understood in the context of Burmese culture, in which people live in close proximity and often with extended family, making the notion of a truly private space in Myanmar uncommon. Stakeholders note that this lack of familiarity with the concept carries over into the digital space.
- **Lack of user concern about privacy**: There is, therefore, a lack of understanding of the importance of the right to privacy online, the basic steps users should take to protect it, e.g. using passwords to protect their online accounts and information, and the consequences of a failure to protect one's own privacy e.g. posting personal information such as bank details online.
- **Lack of awareness on appropriate protections on social media**: Users on social media were observed sharing sensitive personal data including bank statements and checks for donations or even more sensitive information about health status without appropriate protections. Users reported being unaware of how to configure privacy settings in their social media accounts. Users also reported being unaware of how to report on content on social media.
- **Lack of policies or clear communication of policies**: Data retention policies were absent, or in some cases not clearly communicated to the customer/user even when internally present (e.g. 5 years for retention of customer data on paper).
- **SIM Card Registration:** The Ministry of Communications and Information Technology (MCIT) has mandated a system that in theory requires an ID, which is recorded, to buy a SIM card. However in practice, people use their own ID and buy multiple SIM cards for their friends and family members. People have raised concerns regarding data protection and their ID being associated with another user's activity incorrectly. It was noted that in many other countries (e.g. Thailand and India), people are not required to show IDs or register with their IDs to purchase SIM cards.

Data Protection

Human Rights Implicated: Right to privacy

Field Assessment Findings

- **Physical protection of data**: There was variation in the level of access control in place for businesses with data centers. Some businesses logged visitors to data centers, while others had multiple levels of security in place (biometric such as a fingerprint reader, access card, and close circuit television).
- **Protection of data in case of emergencies**: Data backups or disaster response

policies were mostly absent. One bank maintained a data centre for production and a data centre for disaster recovery.

- **Protection of data from unauthorised access within the company**: Role-segregation varied among businesses collecting customer's personal data. One bank segregated employees conducting a 'Know Your Customer' check (where basic information was provided, such as a National Registration Card) from employees conducting financial transactions.
- **Affordability of data protection**: Many businesses used pirated software for internal business functions including email which presents a data protection risk. Small and medium size businesses complained about the cost of buying licensed software.
- **Lack of policies or clear communication of policies**: Data retention policies were absent, or in some cases not clearly communicated to the customer/user even when internally present (e.g. 5 years for retention of customer data on paper).

Myanmar Good Practice Examples:

- Companies are beginning to conduct threat and vulnerability assessments across their applications, network, and infrastructure on an ongoing basis to test the security of the data held in their systems. One bank uses two separate companies to perform assessments (one local and one international).

C. Privacy: Recommendations for ICT Companies

General

- **Understand contextual risks around Myanmar's history and Government action**: Given Myanmar's historical legacy of Government surveillance and information control, coupled with ICT policies and laws that are not aligned with international human rights standards, there exist significant risks for violation of ICT user rights to protection of privacy and anonymity. There are also risks for any ICT company that may be implicated in such violations. Risks related to the violation of the right to privacy in Myanmar with respect to Government actions can be categorised into at least two separate but closely related areas of concern:
  - Government monitoring and surveillance of user activity and content; and
  - Government access to user-identifying information (See Chapter 4.4 on Surveillance).
- **Use company procedures to plug gaps in the Myanmar legal framework:** As Myanmar currently has no legal requirements for mandatory protection of data of ICT users, this means that the protection of personal data is left to individual companies or Government departments, if at all. Sectors such as ICT or the financial sector are likely to be more aware of the importance of data protection. Companies in these sectors may have their own policies and procedures, or industry-specific standards to assist in developing systems and policies. But other companies will also need to develop systems to protect personal information, as well as externally available policies to inform customers about how their data is being handled (see next point).
- **Develop and implement appropriate policies and procedures to safeguard data privacy**: Companies in the ICT value chain, which often collect and store a large amount of personal information about their users, need processes and policies in place to ensure they protect user information. These must be clear about how they will collect, store and share user information with third parties, and under what circumstances the Government (or others) can have access to information or intercept communications. This information would usually be set out in a company's 'privacy

policy'. This policy should be written in easy-to-understand language, spelling out the implications of when the user's data would be shared, with whom, and why. They should be clearly made known to all staff, particularly those with accessnto sensitive data, and the sanctions for breaching them known. The International Standards and Guidance in section D below set out what issues to address when developing their policies and systems.[354]

- **Ensure that businesses' terms and conditions or privacy policies are publically available** so users or customers are aware of what personal data may be collected or shared. The policies should be available in Burmese and local languages. Putting in place robust data protection standards is a good way for local companies to show they are ready to meet data protection requirements from business partners, trading partners and users.

Web Based Services

- **Develop and promote privacy controls**: Overall digital literacy in Myanmar remains low. Many users are interacting with web-based services for the first time. Some international companies have controls in place that allow a user to manage his/her 'digital footprint' online in addition to their broader online experience. A large majority of users in Myanmar are not familiar with these features. On social media, privacy management controls allow the ability to selectively share or restrict information, including access to photographs, contact information or profile accessibility (e.g. public and private settings). For email communication such as newsletters or mailing lists, this involves the ability to unsubscribe or customise subscription settings. Companies need to raise awareness of these features through appropriate media and ensure these features are available in local languages.
- **Develop and promote content-reporting mechanisms**: Abusive or offensive content can violate a user's privacy. Larger social media platforms now maintain community standards, which outline acceptable use online, while also providing guidance to users on how to address violations of these standards in the case of prohibited content or behaviour. Content reporting mechanisms allow users to report abusive or invasive content to platform moderators. For first time users, understanding how and when to report content is a critical part of ensuring a safe experience online. Similar to privacy controls, companies must raise awareness of these features through appropriate media, and ensure that community standards and reporting tools are available in local languages[355].

D. Relevant International Standards and Guidance on Privacy Issues

Relevant International Standards:

- Asia Pacific Economic Cooperation Group (APEC) 2005 Privacy Framework
- EU Data Protection Directive 95/46
- EU Directive on Privacy and Electronic Communications 02/58

[354] See for example, European Commission, "ICT Sector Guide on Implementing the UN Guiding Principles on Business and Human Rights" (2013), pg. 21, 45-46.

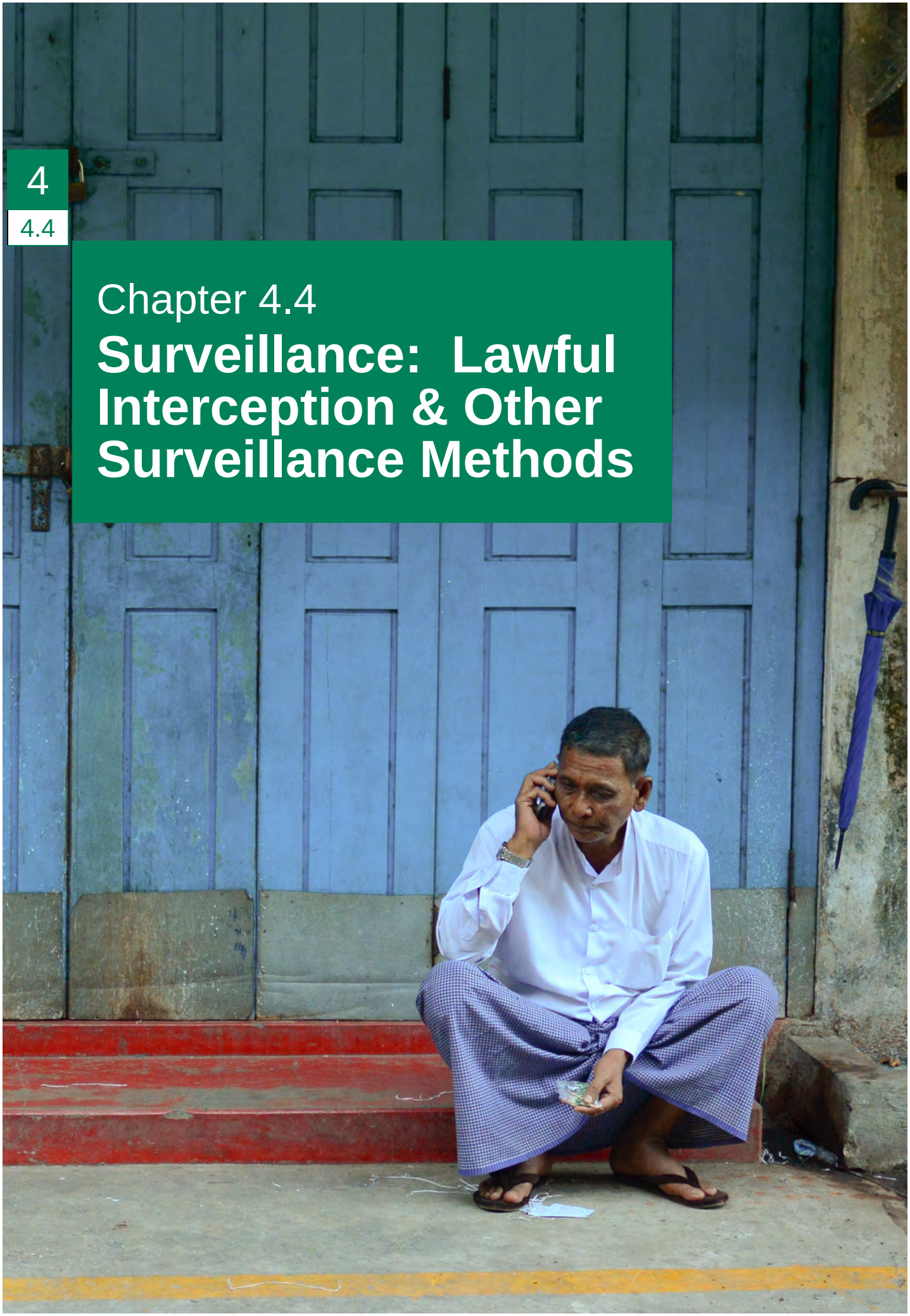
[355] In September 2015, Facebook launched a Burmese version of its community standards 'Facebook rules get local to tackle abuse', Myanmar Times, 10 September 2015

4

4.4

Chapter 4.4

Surveillance: Lawful Interception & Other Surveillance Methods



4
4.4

Chapter 4.4

Surveillance: Lawful Interception & Other Surveillance Methods

In this Chapter:

A. Context

Lawful Interception and Other Surveillance Methods

Governments have legitimate reasons to initiate surveillance of a person's communications i.e. intercept or monitor the communications of certain individuals or organisations. For example, the target may be legitimately suspected of planning to commit or having committed a serious crime, such as a terrorist act. There are two ways a person's communciations can be put under surveillance:

- Interception of the content of communications in real time (known as lawful interception); or
- Access to other, historical user data (known as 'communications data').

Lawful interception is permitted in most countries under legal statute in order to assist with criminal investigations, prosecute serious crime, or prevent national security emergencies. Usually, a telecommunications operator collects intercepted communications of private individuals or organisations, and then provides law enforcement officials with access. Lawful interception refers to the interception of, or access to, a person's communications in real time, as the communication is taking place.

- ***Content*** refers to what was said during a phone call or what can be read in the content of an email or other type of digital message. Interception of content,

depending on the country, usually requires that law enforcement authorities seek a judicial warrant from a court or an executive warrant signed by a senior government official, an important procedural safeguard to protecting the rights of those under scrutiny. (See the Annex to the Recommendations for more information).

In addition to this, authorities may require access to communications data, which is generated as a person uses communications services. This is often known as the 'who, where, when and how' of a communication. With the many different ways to communicate electronically currently in existence, there is a much greater array of data and interactions that can be collected and therefore demanded by law enforcement authorities.

- ***Communications Data*** (this sometimes referred to as metadata but will be described as communications data in this SWIA) is basically everything but the content. It includes telephone numbers of both the caller and the recipient, the time and duration of a call, unique identifying numbers (each subscriber is allocated one, as is each mobile device), email addresses, web domains visited and location data. This information is important as it builds up a detailed picture of a person's life and movements. Often intercepting the content of a call or email is not necessary. In contrast to content, there are often weaker legal protections around interception of stored communications data.

Intercepting communications is an intrusive process into someone's privacy. That is why any such intrusion should be governed by a strict legal framework to prevent arbitrary violations of privacy.

Legal Requirements

The Annex to the Recommendations provides more detailed recommendations on the kinds of considerations any government, including the Myanmar Government, should take into consideration in establishing its procedures for lawful interception or other forms of communications surveillance at each step of the process. These steps include the authorisation process, oversight and remedy procedures for lawful interception, and other communications surveillance, to ensure that the procedures and practice are in line with international law.

Technical Requirements

Telecommunication systems or networks in most countries must include, by law, the technical capability to intercept communications. For example, providing the technical means for interception is a legal requirement for European companies under a *1995 EU Resolution on Law Enforcement Operational Needs with respect to Public Telecommunication Networks and Services,*[356] which allows lawful interception to assist law enforcement in investigating and preventing crime.

In order for communications to be intercepted, the telecommunications system needs to be configured in a specific technical way according to a set of standards. The European Telecommunications Standards Institute (ETSI)[357] (one of many industry-led technical standardising bodies worldwide) has taken the lead in producing globally applicable

[356] Council of Europe (1995) "Council Resolution on law enforcement operational needs with respect to public telecommunication networks and services" (20 June 2001).
[357] See European Telecommunications Standards Institute (ETSI) (last accessed August 2015).

standards for ICTs, including lawful intercept requirements. ETSI defines lawful interception as:

> *"A security process in which a service provider or network operator collects and provides law enforcement officials with intercepted communications of private individuals or organisations."*[358]

It is not yet clear or certain which technical standards Myanmar will be using to implement the technical requirements of lawful interception.

Mass Surveillance

In contrast to lawful interception, mass surveillance is understood to refer to the bulk access and/or collection of many users' communications without prior suspicion of criminal activity by the individual targets. Therefore mass surveillance involves no individual target, no prior suspicion, is not time bound and due to the technology employed, is potentially limitless. In contrast to technology provided for lawful interception, much of the technology that allows mass surveillance is unregulated. The adoption of mass surveillance technology thus impinges on the very essence of the right to privacy. [359]

Products that Facilitate Surveillance

- ***'Dual use' technology*:** 'Dual use' is a legal term applied to products, services or technology that can be used for both military and civilian purposes. In the ICT sector, it can apply to technology that can be used for commercial functions, but may also contribute to infringements on human rights. For example, a technique called 'Deep Packet Inspection' (DPI) was developed to analyse network traffic to make sure the network runs smoothly. However, it is also capable of reading emails and governments wishing to conduct unlawful surveillance can abuse this. Many states known to censor the Internet also use DPI.[360] In January 2012, the European Union banned DPI exports to Syria because of the monitoring and interception capabilities, as it was thought they were being used against dissidents.[361]
- ***Unregulated technology*:** There is growing concern that an increasing number of companies may be selling technology that goes beyond regulated, targeted and controllable interception of individuals under prior suspicion. It is currently considered by many experts to be 'single use', because it is difficult to justify a legitimate use for technology that is capable of intruding so much into a person's correspondence and home. There is evidence that some governments are using the technology to track and detain political dissidents as part of a wider pattern of intimidation.[362] Examples

[358] Ibid, "Lawful Interception".
[359] See: UN General Assembly, "Promotion and protection of human rights and fundamental freedoms while countering terrorism*, A/69/397 (23 September 2014).
[360] Ben Wagner, Ludwig-Maximilians-Universität München and Universiteit Leiden, "Deep Packet Inspection and Internet Censorship: International Convergence on an 'Integrated Technology of Control" Global Voices Advocacy (2009).
[361] EU Council, "Regulation No. 36/2012 concerning restrictive measures in view of the situation in Syria and repealing Regulation (EU) No 442/2011" (18 January 2012) Annex V
[362] Citizen Lab, "From Bahrain With Love: Finfisher's Spy Kit Exposed" (2012); Electronic Frontier Foundation (EFF), Kidane Vs Ethiopia (last accessed August 2015).

include malware[363] that infects a target's computer and switches on webcams and microphones on devices, and zero-days[364], which exploits vulnerabilities in a computer application to enable hacking of communications, therefore reducing digital security for many others using the same application. Companies selling these technologies often try to portray these products as having the same status as statutorily mandated (and regulated) 'lawful intercept' functionality – often simply because they are sold to a government purchaser. However experience has shown that some governments are using these technologies quite specifically because they are not regulated and to avoid following lawful interception procedures.[365] With these tools, surveillance is not limited to those within a country's borders, which puts exiles or the diaspora overseas at risk of intrusive surveillance.[366] Companies who sell this type of technology are increasingly being targeted by law suits and other legal actions.[367]

Concerns about Surveillance and the ICT Sector

Under international human rights law[368], individuals are protected from any unlawful and arbitrary interference with their privacy, family, home, or correspondence. The act of surveillance, whether physical (such as a house search) or of a person's communications (such as monitoring phone calls and emails) is an inherently intrusive act and risks violating a person's privacy. In addition, surveillance of person's communications can limit the exchange of information and ideas resulting in a 'chilling effect' on freedom of expression, as people are less likely to express themselves freely if they know they are being observed or monitored.

Intercepting communications is under particular scrutiny by international organisations, civil society groups and governments due to the impact of surveillance on privacy and other human rights such as the right to receive and impart information. [369] The same technology that can help law enforcement prosecute criminals may also be misused by authorities, such as when specific groups (opposition parties, human rights defenders, ethnic, religious or sexual minorities) are placed under surveillance for the purpose of intimidating, persecuting and silencing them. There is evidence in some countries that the technology is being used to track and detain political dissidents as part of a wider pattern of intimidation, often with negative consequences or harm to the individuals.[370]

---

[363] Software that is created and used to gain access to private computer systems, disrupt computer operations and/or gather sensitive information. Malware includes computer viruses, "Trojan horse" software and "worms".
[364] An attack on vulnerability in a computer application or operating system that developers have not yet addressed.
[365]Citizen Lab, "Shedding Light on the Surveillance Industry: The Importance of Evidence-based, Impartial Research" (20 December 2013).
[366] For example, there is evidence that the government of Ethiopia is using surveillance technology to target the diaspora overseas who may be critical of the government. Ethiopians living in the UK, US, Norway and Switzerland have been targeted with malware, resulting in an illegal wire-tapping case in the US. See Electronic Frontier Foundation (EFF), Kidane Vs Ethiopia (last accessed August 2015) and Reporters Without Borders "Enemies of the Internet" (2014).
[367] For examples of lawsuits and other official complaints, see OECD Watch and the Business and Human Rights Resource Centre.
[368] International Covenant on Civil and Political Rights, Article 17.
[369] See for example the Global Conference on Cyberspace 2015, the Global Commission on Internet Governance, the work of the United Nations and international civil society organisations such as Privacy International, Electronic Frontier Foundation, Citizen Lab, Access, and many local civil society organisations.
[370] See for example: Freedom House, "Freedom on the Net" (2013) details a particular example from Sudan:

Being able to locate a mobile phone also means being able to locate the person carrying the mobile phone, which is potentially a powerful tool for surveillance. It is important to have access to such information in emergency responses, such as abduction or identifying survivors in a natural disaster area. However mobile phone technology has unfortunately become increasingly dangerous for activists in some countries.

It is therefore critical that any intrusion into a person's privacy through the interception of communications is subject to legal process and includes protection for human rights. In countries where the relevant legal framework on lawful interception is absent or deficient, when there is a case of a misuse, companies within the ICT value chain that have had a role in that process (network providers, vendors, operators, over the top service providers) are often accused of contributing to the abuse of human rights through its operations. This may involve invasions of privacy or in some cases even more severe abuses such as torture. Some companies may actively assist the government in carrying out arbitrary surveillance by allowing secret access to their servers (often called a 'back door'). If the government responsible for the misuse is perceived to be repressive, this may increase scrutiny by human rights groups.

History of Surveillance in Myanmar

The former military government in Myanmar established an intrusive surveillance regime for many years, both online and offline, in order to suppress criticism and dissent and restrict access to information. The fear and threat of surveillance was part of life, especially for members of opposition political parties, student activists, and ethnic minorities in armed conflict areas.

Physical Surveillance

Under the former military government, intelligence agencies, some of which were originally established under British colonial rule, proliferated. Multiple organisations were charged with keeping people under surveillance. Intelligence activities expanded rapidly following the 1988 coup d'état which re-established military rule after its suppression of the nationwide pro-democracy movement. The hierarchy and structure of the intelligence agencies changed throughout the 1980s, 1990s and 2000's as the military government imprisoned or purged various members of the intelligence community. Before the reform process began in 2011, Myanmar's intelligence agencies played a consistent role in gathering information on real or impugned critics, in suppressing dissent, and in arresting and interrogating suspects.

The *Village Act* and *The Town Act* required everyone to report the identity of overnight guests to local officials, who could refuse "*permission*" for houseguests. The law was enforced by periodic household inspections by authorities, often accompanied by Special

---

"The activist Mohamed Ahmed switched off his phone for a few days in early July 2012 to avoid arrest while in hiding from the NISS [National Intelligence and Security Service]. When he turned his phone back on as he was walking home to see his family, NISS officials roaming his neighbourhood managed to track his location based on the nearest telecommunications tower and arrested him later that night." pg. 14.

Branch agents, and mostly at night. It has been reported that these inspections were used as an opportunity to monitor, harass or arrest political activists and inspections increased during the pro-democracy uprisings in 1988, 1998 and 2007. [371]

In addition to intelligence agencies, a wide network of informants attached to various official groups operated throughout the country. A 2007 Human Rights Watch report stated that this group of informants systematically began to track down activists and organisers of the 2007 protest movement, often known as 'the Saffron Revolution'.[372]

Telecommunications surveillance

As early as 1990, reports surfaced that telephone calls and faxes were being monitored. A computer centre was reportedly set up which carried out more "*politically focused*" intelligence gathering, including monitoring communications of opposition groups both within and outside Myanmar.[373] This timing coincided with exiles fleeing the country in the wake of the 1988 crackdown on the pro-democracy movement and setting up exile media groups, newsletters and websites to report on the situation inside Myanmar.

It has also been suggested that wiretapping of phone conversations was common, in particular to identify leaders of activist movements. Once leaders had been identified, this would be followed up with a night-time "*inspection*".[374]

Online surveillance

Despite Myanmar's low Internet penetration, the Internet and its users were reportedly under near constant surveillance as the first Internet connections were established around the year 2000. For citizens wanting an email account, the only choice was to pay for an email account supplied by Myanma Post and Telecommunications (MPT), a state run telecommunications company. Users assumed these accounts were closely monitored. However, it is difficult to establish exactly what technology enabling online surveillance was purchased and utilised by the government.[375]

---

[371] Fortify Rights, "Midnight Intrusions: Ending Guest Registration and Household Inspections in Myanmar" (2015), pg 12.
[372] A 2007 Human Rights Watch report found the local ward Peace and Development Councils, the Union Solidarity and Development Association (a movement supporting the military government, disbanded in 2010) and Swan Arr Shin (a local paramilitary group) all contributed informants who conducted surveillance activities and gathered intelligence. Human Rights Watch, "Crackdown. Repression of the 2007 Popular Protests in Burma" (2007), pg. 83.
373 Brian McCartan, "Myanmar on the Cyber-Offensive" *Asia Times* (1 October 2008).
[374] Fortify Rights, "Midnight Intrusions: Ending Guest Registration and Household Inspections in Myanmar" (2015) pg. 31.
375 See for example: Joe Havely, "When States Go To Cyber-War" *BBC News Online* (16 February 2000). The BBC reported that the government had acquired surveillance capabilities by borrowing equipment from other countries: *"Using monitoring equipment loaned by the government of Singapore, analysts say the junta has been able to track online critics of the regime."* A 2005 Open Net Initiative report on internet filtering in Myanmar also mentions online surveillance, reporting that the state *"maintains the capability to conduct surveillance of communication methods such as email…"* Open Net Initiative, "Internet Filtering in Burma in 2005: A Country Study" (2005), pg. 4. A 2007 Berkman report stated that the military government was buying surveillance technology from an un-named U.S company. Chowdhury, M. Berkman Centre for Internet and Society at Harvard University, "The Role of the Internet in Burma's Saffron Revolution" (2008) pg. 13.

Although the Internet penetration in the 2000's was less than 1%, activists were quick to make use of the limited service they had. Despite pervasive surveillance, the 2007 Saffron Revolution came to global attention thanks largely to activists anonymously uploading images and video to websites such as YouTube, which were then picked up by international news agencies, as journalists were prevented from entering the country. Some managed to email images to friends outside Myanmar to upload onto sites such as the Democratic Voices of Burma (DVB), or smuggle content out of the country on USB sticks. This was the first time in the country's history that ICTs played a significant role in disseminating information about protests and the security forces' violent suppression of such protests. In addition, the 2009 documentary Burma VJ[376] featured some of the video footage and images, and revealed that many of the activists involved had either been arrested and punished, or fled Yangon.

Surveillance of Cybercafés

Public Internet access inside Myanmar was previously only possible from a few Internet cafes in Yangon and Mandalay, the two largest cities. The first cybercafé opened in Yangon in 2002[377]. From around 2006, cybercafés required a license to operate from the Myanmar Information Communications Technology Development Corporation (MICTDC). They were licensed as Public Access Centres (PACs) managed by Myanmar Info-Tech, a state-owned company. Regulations[378] stated that users had to register at the cybercafé before accessing the Internet and café owners had to take screenshots of user activity every five minutes, delivering CDs containing these images to MICTDC at regular intervals.

In 2008, the Open Net Initiative reported: "*Anonymous Internet use is impossible; cybercafé licences require that patrons register their name, identification number, and address to gain access. Opportunities for anonymous communications are further hampered by the state's ban on free email sites such as Hotmail and Yahoo! mail."*[379]

[376] Anders Østergaard, *Burma VJ: Reporting From A Closed Country* (2008). Among other awards, the film was nominated for the Academy Award for Best Documentary Feature in 2010.
[377] Reporters Without Borders, "Internet Under Surveillance 2004- Burma" (2004).
[378] "Public Access Center Regulations by Myanmar Info-Tech" (2006). See an unofficial English translation by the Open Net Initiative (ONI), which includes a link to the original version in Burmese.
[379] Ibid, pg. 11

Surveillance since the 2011 Reform Process

Little is known about intelligence gathering practices in Myanmar since 2011.[380] It is believed that at least two intelligence agencies are still operational – the Military Affairs Security (MAS) and the Special Branch of the Myanmar Police Force[381] . In 2011, *Irrawaddy* reported that a new intelligence unit had begun to operate, staffed by military and police officers. It was reported that the new unit would not operate as a separate entity, as intelligence agencies had previously done, and had to reports to "*both military and civilian authorities, as well as administrative officials*". According to the report, the role of the unnamed intelligence unit was to *"investigate the movements of political parties, ethnic armed forces and cease-fire groups, violent domestic actions such as bomb explosions and any matter that affects the state's security and stability, including non-disintegration of the military, and take necessary measures*."[382]

It is unclear which elements of the surveillance apparatus are still operational, but it appears that authorities are still conducting a combination of physical and electronic surveillance by replacing old laws with something very similar, and utilising new technology. For example, in 2011, Reporters Without Borders reported that new updated regulations had been sent to cybercafé owners, *"including a requirement to keep the personal data of all their clients along with a record of all the websites they visit, and make it available to the authorities."*[383]

In 2012, *The Village Act* and *The Town Act* was replaced by The *Ward or Village Tract Administration Law,* which upholds the process of overnight guest registration and inspection. Although inspections have reportedly declined, and more people are ignoring the law as there are no longer the same fears of reprisal, there have been recent crackdowns on student protesters, forcing many to go into hiding.[384] Student's houses have reportedly been "*inspected*" in the middle of the night, had their mobile phones seized and their Facebook accounts hacked.[385]

Reports suggest that surveillance of community leaders, opposition political party members and journalists continue. Some reported being physically followed or enquired after, and some fear their phone conversations are monitored.[386] In 2013 it was reported that the website of the Myanmar news group Eleven Media, was under surveillance. One of its journalists was physically followed by intelligence agents while reporting on the war in Kachin State.[387] Journalists from Eleven Media and others working on Myanmar reported they had received notification from Google, which runs the Gmail email service,

---

[380] Andrew Selth, "Burma's Security Forces: Performing, Reforming or Transforming?" *Griffith Asia Institute, Griffith University, Australia* (2013), pg. 16.
[381] The Hindu, "In Myanmar, Internal Spy Network Lives On" *Associated Press report* (30 July 2013).
[382] The Irrawaddy, "Burma Forms New Intelligence Unit" (3 May 2011).
[383] Reporters Without Borders, "Surveillance of Media and Internet Stepped Up Under New Civilian President" (2011).
[384] Wa Lone and Guy Dinmore, "Student Activists Go Into Hiding After Crackdown" *The Myanmar Times* (20 March 2015).
[385] Ibid
[386] Andrew Selth, "Burma's Security Forces: Performing, Reforming or Transforming?" *Griffith Asia Institute, Griffith University, Australia.* (2013), p17.
[387] Bertil Lintner, "The Military's Still In Charge" *Foreign Policy* (9 July 2013).

that their accounts may have been hacked by "*state-sponsored attackers*".[388] It is unclear if the purpose of these attacks were to gain access to journalist's emails and identify sources, or to stem the flow of information to and from Myanmar. It was also reported that government agents visited cybercafés to "*install some software*", widely believed to be 'keylogging' software, which records and stores keystrokes for later analysis. Some café owners have put up signs warning customers not to use the Internet for "*political reasons*".

It is also unclear what kind of relationship Myanmar's existing intelligence agencies have with foreign counterparts, and what kind of intelligence exchange agreements exist. It is thought that Embassies routinely reported on the activities of the diaspora.[389]

The Legal Framework in Myanmar

There are currently few protections in Myanmar's legal framework to prevent the kind of pervasive surveillance previously conducted by intelligence agencies and about which there is justifiable concern. It is unclear under which legal regime the existing intelligence agencies are operating, what their remit is and how they are exercising their powers. Although Article 357 of the 2008 Constitution does provide for privacy[390], there are no privacy protections in national legislation. The existing legal framework referring to surveillance is vague. Article 75 of the 2013 Telecommunications Law [391] grants unspecified government agents the authority *"to direct the organisation concerned as necessary to intercept, irrespective of the means of communication, any information that affects the national security or rule of law".* Although the clause adds this should be undertaken without impacting the fundamental rights of citizens, there are no further details on the process or privacy protections.

Most states have a specific legal framework in place to govern instances where interception of communications is permitted in real time (lawful interception). However Myanmar currently has no specific legal framework or regulations governing lawful interception, leaving an important gap in the regulatory framework. The MCIT has confirmed its interest in developing a law in accordance with international standards. It has committed to a public consultation of draft lawful interception regulations.[392] One of the current telecommunications operators, Telenor, has stated publicly that they will not respond to any interception requests from law enforcement officials until the legal framework is in place.[393]
The EU has agreed to provide technical support to the Government to develop its regulations in line with human rights. The programme of work will come within the Council

[388] Thomas Fullller, "E-Mails of Reporters in Myanmar Are Hacked" *New York Times* (10 February 2013).
[389] Andrew Selth, "Burma's Security Forces: Performing, Reforming or Transforming?" *Griffith Asia Institute, Griffith University, Australia* (2013), pg. 18.
[390] "*357. The Union shall protect the privacy and security of home, property, correspondence and other communications of citizens under the law subject to the provisions of this Constitution.*"
[391] See unofficial English translation of the Myanmar *2013 Telecommunications Law*.
[392] In November 2013, MCIT published draft proposed rules, stating: *"The Ministry will be drafting other rules and procedures on a variety of issues such as standardization, type approval, and lawful interception in due time. Such rules and procedures also will be subject to a public consultation process."* MCIT, "Proposed Rules for Telecommunications Sector Relating to Licensing, Access and Interconnection, Spectrum, Numbering, and Competition" (4 November 2013), Section I, B5 (pg. 5).
[393] Telenor, "Myanmar sustainability presentation" (19 August 2014), pg. 8 of the transcript.

of Europe programme on cybersecurity, particularly focused on the Council of Europe Convention on Cybercrime.[394] Regulations are needed to govern the use of surveillance to ensure any infringement of privacy rights is legal, necessary and proportionate and the act of surveillance is not abused to cover people who are not suspected of carrying out a crime but whom the government may disagree with.

The Government has already committed to requiring judicial authorisation of any request for lawful interception, which is an important first step. Given the weak state of the Myanmar judiciary, it is clear that any judicial authorities involved in such authorisation processes will require thorough training, both in the technicalities of lawful interception, but also in the importance of the legal safeguards that an independent review represents. See Chapter 4.9 on Stakeholder Engagement and Access to Remedy for a short overview of the judiciary.

The idea of a judicial authority challenging and even denying authorisation to the executive branch to carry out surveillance for what the government claims is a national security issue or emergency, will be an unfamiliar concept in Myanmar. Even in countries with highly developed judicial systems, there is little open scrutiny of the decisions made by judicial authorities on lawful interception. The challenges of establishing a gatekeeping system in Myanmar that respects rights and establishing a proportional, targeted approach to security are therefore significant. The companies involved in executing lawful interception requests may currently be one of the few credible counterpoints in the system. (See Section C providing Surveillance Recommendations for ICT Companies) The Annex to the Recommendations also suggests the main issues for the Government of Myanmar to take into account in developing lawful interception law and procedures.

B. Field Research Findings

Current Status of Lawful Interception in Myanmar

Human Rights Implicated: Right to Privacy, Freedom of Expression

Key Findings

- Many people in Myanmar **grew up under a repressive surveillance regime**, and are familiar with methods of physical surveillance, such as being followed. However, the majority do not know how digital surveillance is carried out and who has access to their data, phone records, etc.
- There is a prevailing **lack of trust** between the public and the government, as well as a belief that the government will not protect or respect citizens' privacy or personal data. There is a feeling among the general public that there is still physical surveillance and that government agencies likely monitor their digital communications.
- There is **no oversight body** (parliamentary or otherwise) for lawful interception, and no clear process in place.
- **There is currently a lack of legal framework for lawful interception:** In May 2015 with support from international consultants, MCIT held an initial "*fact finding*" session, focused on cyber-crime and electronic evidence, in which MCRB participated. The next steps are unclear. In the interim, PTD has requested

[394] Council of Europe, *Convention on Cybercrime* (CETS 185) (2001).

operators comply with requests for data in cases related to human trafficking, terrorism, and drug offenses.

- There are **inconsistent policies for handling data requests from law enforcement.** One operator mentioned that they have an in-house policy regarding lawful interception, allowing them to provide data to the government in serious criminal cases. This operator has a specific department for lawful interception to review requests. Requests must have an authorised signature of Ministry of Communications Information Technology to be reviewed by the operator before providing any data.
- A mobile network operator's regional office noted that little scrutiny is applied when law enforcement requests location data or call records. The information is usually provided.
- One operator has designated **a small internal team** to review the legitimacy of any data requests received from law enforcement.

C. Surveillance and Lawful Interception: Recommendations for ICT Companies

The following section focuses on the use of ICT for surveillance, rather than physical surveillance. (See also Chapter 4.3 on Privacy)

General

- **Understand Myanmar's history**: ICT companies that operate within those parts of the ICT value chain that may be subject to surveillance requests from the Government should understand the extensive historical level of surveillance in the country and its often severe consequences. The population and civil society organisations are therefore justifiably sensitive to the possibility of continued surveillance, and the current lack of appropriate legal safeguards on surveillance.
- **Understand the wider global discussion about surveillance**: Just as foreign companies coming into Myanmar need to understand the historical context around surveillance and its connotations for the population and its customers, local companies also need to understand the wider context of the active, on-going debate around surveillance and its implications for human rights.

Tower Construction

- **Be aware of the possibility of interception and misuse of base stations:** It is possible for other actors to intercept signals sent from cell towers by setting up technology that essentially pretends to be a base station and collects the information[395]. There is some evidence this being done elsewhere to locate activists and political opposition[396]. There are different types of hardware that can act as a base station and enable interception of mobile signals. The devices do not necessarily have to be in the vicinity of the cell tower or real base station to work. Tower

[395] One such example is an International Mobile Subscriber Identity (IMSI) catcher which works by masquerading as a base station, in order to track a mobile phone's location in real time. IMSI catchers are subject to export control in the US and EU.

[396] For example, during the 2014 Euromaidan protests in Ukraine, protestors in the vicinity of one march in the Ukrainian capital Kiev were sent unsigned text messages reading: *"Dear subscriber, you are registered as a participant in a mass disturbance".* Local mobile operators denied sending the message to their subscribers on behalf of the government, and one insisted that the messages were sent from a "*pirate base station*". Heather Murphy, "Ominous Text Message Sent To Protesters in Kiev Sends Chill Around The Internet" *New York Times* (22 January 2014).

construction companies should therefore be aware that their infrastructure may be targeted by actors wishing to illegally intercept mobile phone signals for the purposes of surveillance, impacting both freedom of expression and privacy. When tower construction companies carry out their regular checks and maintenance, they should therefore be especially vigilant for any signs that cell tower or base station equipment has been tampered with.

Infrastructure

- **Do not provide lawful interception services until a legal framework is in place:** Lawful intercept solutions provided as part of the network infrastructure of operators should not be operational until national legal framework and regulations are in place and it is clear which set of technical standards Myanmar will adopt (ETSI standards or another). Without legal safeguards in place, companies requested to take action by the government to action lawful interception may be contributing to human rights violations of the right to privacy and potentially further severe impacts, depending on the action taken by the government once it has secured the information. Vendors should be prepared for such requests and consider through their due diligence processes the human rights risks associated with these transactions. This includes due diligence pre-sale, during the sale in putting appropriate conditions or procedures in place in sale documents or contracts, and in post-sale due diligence.[397]
- **Train operator personnel:** In addition to carrying out the appropriate due diligence, vendors should ensure that equal attention is given to training of operator personnel as part of the sale of technology products, including lawful interception systems. Myanmar staff may not be informed or even consider the wider implications of their actions unless they are provided with specific training.
- **Send clear messages about business relationships**: The opening of the Myanmar ICT market has seen a rush of new companies to the market. Unlike other bigger footprint sectors, smaller ICT companies have far fewer downside risks in entering and exiting markets quickly. Some of the companies selling unregulated surveillance technology market themselves by asserting that their technology can be added to a particular vendor's network as lawful intercept 'solutions' when in fact they provide capabilities that go well beyond what is lawful. Network vendors should publicly distance themselves from these companies, ensuring that their company's logo and name are removed from any marketing literature by such enterprises and by providing a clear message to the Government that they do not condone such products.

[397] See for example guidance on dealing with government requests: European Commission,"ICT Sector Guide on Implementing the Corporate Responsibility to Respect Human Rights" (2013), pg. 32-33. IHRB, "Human Rights Challenges for Telecommunications Vendors: Addressing the Possible Misuse of Telecommunications Systems. Case Study: Ericsson" (2014).

Telecommunications Operators

- **Challenge lawful interception requests without appropriate legal safeguards**: Operators are the party in the ICT value chain that receives any request from the government for interception of the content of phone calls and emails, or access to other information such as user/subscriber information and records. As noted above, Article 75 of the *2013 Telecommunications Law* includes a sweeping provision on surveillance. Subsequent regulations for assistance with real time surveillance are not in place. One of the current telecommunications operators, Telenor, has stated publicly that they will not respond to any interception requests from law enforcement officials until the legal framework is in place.[398]. Even when such regulations are in place and even assuming that they are aligned with international law, given the history and current state of development of Myanmar's judiciary, the operators may be one of the few credible actors in the process capable of challenging overly broad or inappropriate requests.
- **Develop robust systems for responding to government requests** to avoid over-complying with illegal requests.[399] Such a company system could include for example, ensuring that there is a process in place to review each request submitted; a designated contact person in the company; a list of government departments authorised to request information; a requirement that the request to the company must be made in writing (or at least followed up in writing if such a request is made during the course of an emergency); challenging requests that do not comply with the law or human rights standards; developing criteria for escalation of requests; and where feasible, notifying affected customers or users. See the Annex to the Recommendations for further information.
- **Be transparent about the number of requests for surveillance:** Out of three telecommunications operators in Myanmar, only one telecommunications operator issues a transparency report disclosing interception requests from law enforcement, including cases the company has complied with.

'Over the Top' Companies (National and International)

- **Challenge requests for user information without appropriate safeguards:** Like telecommunications operators, over the top companies which store data on servers inside Myanmar need robust systems for screening and responding to such requests to ensure that they do not contribute to potential human rights violations. [400] While certain information about a user may be publicly accessible, for example by looking at a public profile on social media, companies store much additional personal information about their users, such as names, addresses, contact numbers and private online conversations. Depending on the service, companies will also have a lot of information about a person's movements, how they spend their time and money and the opinions they hold, which could potentially be used in gathering intelligence. Over the top companies may also be requested to turn over user information by the Government as part of its surveillance activities.

---

[398] Telenor, "Myanmar sustainability presentation" (19 August 2014), pg. 8 of the transcript.
[399] See for example guidance on dealing with government requests: European Commission, "ICT Sector Guide on Implementing the Corporate Responsibility to Respect Human Rights" (2013), pg. 44-45 and the Telecommunications Industry Dialogue.
[400] See for example guidance on dealing with government requests: European Commission, "ICT Sector Guide on Implementing the Corporate Responsibility to Respect Human Rights" (2013), pg. 44-45 and the Global Network Initiative (GNI), "Principles and Implementation Guidance" (last accessed August 2015) on dealing with government requests.

- **Establish clear company terms of service** which are understandable to local users, setting out what information the company collects and stores and under what legal justification that information can be accessed by the government.

Software

There are many different kinds of software, but the focus of this chapter is the tools that can aid surveillance; that is, the software that can be added to a telecommunications network in order to increase surveillance capabilities.

- **Do not sell surveillance software to Myanmar.** Surveillance software is not a new issue for Myanmar. As far back as 2000 it was reported that Burmese exiles were being targeted with malware. However, this kind of technology has advanced rapidly in recent years. While the goal of the military government in the 2000's may have been to stop information exchange or communication by freezing computers or taking websites offline, viruses, malware and spyware contained in infected emails are now capable of doing much more intrusive surveillance. Companies selling surveillance equipment, whether 'off the shelf' or bespoke services are under particular scrutiny due to the clear implications for human rights.[401] Sellers of such technologies often justify their use by saying they are intended to support law enforcement or protect the public welfare (e.g. through protecting against terrorist activity), but they often can also be used to facilitate human rights violations by the purchasers. There are currently debates in Europe about tightening export controls to restrict the kinds of surveillance technology that can be exported, particularly to governments with a poor human rights record.[402] Due to the lack of legal framework around surveillance, interception and privacy protections, Myanmar should be a no-go area for companies selling surveillance technology.[403]

D. Relevant International Standards on Surveillance and Lawful Interception

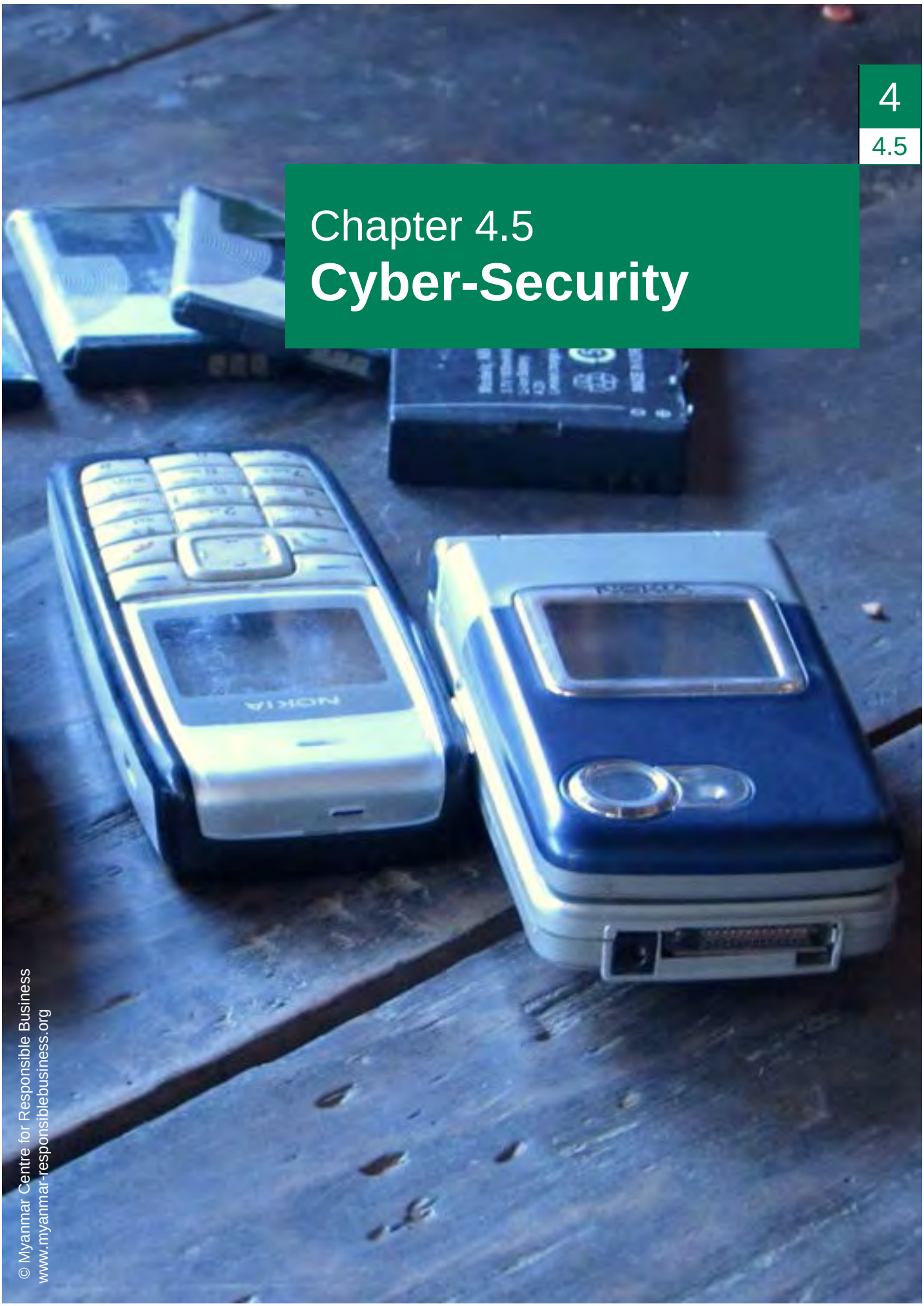
Relevant International Standards:

- International Principles on the Application of Human Rights to Communications Surveillance (Necessary and Proportionate Principles) 2014

Relevant Guidance:

- Universal Implementation Guide for the International Principles on the Application of Human Rights to Communications Surveillance (2015)
- Electronic Frontier Foundation (EFF) Human Rights and Technology Sales: How Corporations Can Avoid Assisting Repressive Regimes (2012).

[401] See commentary by the Chair of the OECD Working Party on Responsible Business Conduct, "Responsible Business Conduct in Cyberspace" (30 April 2015).
[402] For example, the Stockholm International Peace Research Institute (SIPRI) is working on a data collection program in support of the European Commission's ongoing impact assessment for the review of the EU dual-use regulation.
[403] For more guidance, see Tech UK "Assessing CyberSecurity Export Risks" (2014).



Chapter 4.5

Cyber-Security

Chapter 4.5
Cybersecurity

4
4.5

In this Section:

A. Context

Cybersecurity

A safe and secure Internet is a global Internet governance priority. There are many threats that can undermine the security and stability of cyberspace, impacting governments, business, civil society groups and individual users. Cyber-attacks, or cybercrime, can come in many forms, resulting in loss of services or loss of control over services, stolen personal information (such as credit card details), fraud and identity theft and receiving a high volume of spam messages. A range of actors execute cyber-attacks, including: national governments, criminals, business, hacker groups or individual hackers[404]. Attacks can be carried out by spreading computer viruses, denial of service attacks (DDoS)[405], phishing[406], or hacking.

Governments, business, civil society groups and individual users can all be victims of cyber-attacks, and there have been some high profile examples in recent years. Estonia suffered a three-week long cyber-attack in 2007 that disabled banks, companies, government ministries and newspapers. Experts from the North Atlantic Treaty Organisation (NATO) had to be called in to help the country defend and rebuild its cyber capabilities.[407] In 2014, Sony Pictures systems were hacked, reportedly by North Korea, resulting in a leak of employee details, employee emails and yet-to-be-released films.[408]

Encryption[409] is the technique by which data (when in transit or when at rest on devices) is scrambled to make it unreadable without using specific passwords or keys. It is important to keep personal data safe from criminals and therefore extremely important for the

[404] A hacker is someone who seeks and exploits weaknesses in a computer system or computer network. Sometimes this can be for malicious intent (known as 'black hat' hackers) or it can be dome for ethical reasons, such as helping make services more secure (known as 'white hat' hackers)
[405] A *Distributed Denial of Service* (*DDoS*) attack is an attempt to make an online service unavailable by overwhelming it with traffic from multiple sources.
[406] Phishing is the act of sending an email to a user falsely claiming to be an established legitimate enterprise in an attempt to scam the user into surrendering private information that will be used for identity theft.
[407] Ian Traynor, "Russia accused of unleashing cyberwar to disable Estonia" *The Guardian* (17 May 2007).
[408] Vlad Savov, "Sony Pictures Hacked: The Full Story" *The Verge* (8 December 2014).
[409] A recent report by the UN Special Rapporteur on Freedom of Expression, David Kaye, defines encryption using the SANS Institute definition from the Sans Institute, "History of Encryption" (2001), a mathematical "*process of converting messages, information, or data into a form unreadable by anyone except the intended recipient*".

Internet economy. With encryption comes security of user data, authentication, confidentiality and consumer trust in services. People undertake an increasing amount of legitimate activities over the Internet that involve personal information, such as banking, buying and selling goods, filing tax returns, and so on. Without encryption, e-commerce would never have taken off and cannot survive.

Table 39: Definitions of Cybersecurity

Definitions of cybersecurity differ slightly according to international and regional bodies, but the common theme to describe cybersecurity is protecting:

- The availability of services
- The integrity (security) of network infrastructure
- The protection of private information

Cyber security is defined by:

- **the International Telecommunications Union** (ITU) (and cited by ASEAN) [410] as: …*the collection of tools, policies, security concepts, security safeguards, guidelines, risk management approaches, actions, training, best practices, assurance and technologies that can be used to protect the cyber environment and organisation and user's assets..*"[411]
- **the European Union** as: "…*the safeguards and actions that can be used to protect the cyber domain, both in the civilian and military fields, from those threats that are associated with or that may harm its interdependent networks and information infrastructure. Cyber-security strives to preserve the availability and integrity of the networks and infrastructure and the confidentiality of the information contained therein*."[412]
- **the Freedom Online Coalition** as: *"… the preservation – through policy, technology, and education – of the availability*, confidentiality* and integrity* of information and its underlying infrastructure so as to preserve the security of persons both online and offline*." *as defined by ISO 27000 standard.[413]

Concerns about Cybersecurity, Human Rights and the ICT Sector

Recent research by Citizen Lab has shown that CSOs around the world face the same threats of attack as governments and business, but have fewer resources to fend off a cyberattack.[414] The attacks on CSOs are intended to undermine communications, by taking websites offline or disrupting other communications.

Encryption is not just important for safe transactions, it is also important for human rights defenders[415] and people at risk, so that they are able to communicate without the fear of their confidential communications being intercepted arbitrarily by intelligence agencies.[416]

[410] ASEAN, "Joint Ministerial Statement on ASEAN Cybersecurity Cooperation" (2013).
[411] ITU, "Overview of Cybersecurity" (2008).
[412] European Commission, "Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace (2013), footnote 4.
[413] Freedom Online Coalition, "WG 1 – An Internet Free and Secure" (last accessed August 2015).
[414] Citizen Lab, "Targeted Threats Against Civil Society" (2015).
[415] New technology is emerging to support field data collection by civil society organizations working in sensitive communities. See Martus.
[416] Various tools are available to provide human rights defenders and people at risk with higher levels of encryption. The Tor Browser is a web browser that allows users to browse the internet anonymously. Additionally, Pretty Good Privacy (PGP) can be used for encrypting email messages.

However some governments are already specifically targeting civil society groups because they use encryption and Internet security techniques. One of the charges against the jailed Zone 9 bloggers in Ethiopia is their use of encrypted communication and participating in trainings on Internet security.[417] Such training is provided by the well-recognised Berlin-based organisation Tactical Technology Collective, which has developed the popular tool, *Security In A Box*, a publicly available resource used by thousands of human rights defenders worldwide.[418]

Cybersecurity attacks can jeopardise user privacy. Companies are increasingly attractive targets for cyberattacks, jeopardising the confidentiality, availability and integrity of network systems and personal data.

Myanmar Context

As technology becomes increasingly personal and prevalent in Myanmar life, services will evolve and risks will increase. Personal data will be stored, transmitted, and accessed by smart-phone applications, or web-applications for services such as online-banking, e-commerce, or e-government. International examples demonstrate that failing to maintain the integrity and security of these services has severe implications. In Myanmar, some have described recent ATM fraud in Myanmar as the first wave of cybercrime as networked services expand.[419]

Figure 4: Breakdown of cybersecurity incidents in 2013

As of September/2013

Type of Incident	No. of Incident
Scanning	2
DoS	14
DDoS	4
Malware	8
Exploiting Known Vulnerability	18
Login Account	1
Unauthorized Use	2

Source: 2013ASEAN-Japan Symposium on Cyber Security "ICT Usage & Cyber Security Issues in Myanmar" (October

Figure 4 above shows a breakdown of incidents reported by the Myanmar Computer Emergency Response Team (MMCERT) as of September 2013.

[417] See Trial Tracker Blog, "Contextual translation of the charges of the Zone9 bloggers" (19 July 2014) and Tactical Technology Collective, "Tactical Tech's and Front Line Defenders' statement on zone 9 bloggers" (last accessed August 2015).
[418] See Burmese language version of Security in a Box.
[419] See The Irrawaddy "Foreigners Charged over ATM Scams in Rangoon" (November 2014). In November 2014 thieves used cloned ATM cards to steal 25.2 million Myanmar Kyats across Yangon.

Phishing

Simple "phishing", where fraudulent emails are sent with the intention of extracting money or obtaining personal information such as bank details, have been seen in Myanmar for over a decade. Myanmar recipients have been taken in by fake 'You have won the lottery!' emails, and letters from the President of the World Bank.

DDoS Attacks

Myanmar suffered a huge DDoS attack in 2010, just before the election. The main Internet service provider, MPT, was overwhelmed and the attack essentially took the country offline. The attack was discovered by the research organisation Arbour Networks, which reported the attack was larger than the 2007 attack on Estonia, but could not establish its origin. Speculation ranged from placing blame on the Government of Myanmar in order to disrupt the election, to external hackers with unknown motives.[420]

In 2011, Irrawaddy reported they had been victim to likely DDoS attacks, forcing the website to be temporarily shut down. Hackers also penetrated Irrawaddy's central server and planted false new stories on the website's front page, claiming a popular Burmese actress had died. It was also suspected hackers had gained access to confidential information stored on the server, such as the identity of sources. The Irrawaddy hired European security specialists to investigate the attacks, who traced to an IP address in London.[421]

A variety of hacker groups have been reported as active in Myanmar. These groups include the Kachin Cyber Army, Bangladeshi Cyber Army and Indonesian Cyber Army. [422] Blink Hacker Group has also been reported to be active.[423] Attacks have typically included website defacement or service takedown via a denial of service attack (DDoS).[424]

Targeting Burmese Exiles with Malware

Throughout the 2000's, there were repeated reports that Burmese exiles were being targeted by the state with malicious software, or "malware", by concealing computer viruses in emails, sent to targets with titles such as 'Happy Birthday' or 'I need help'. The purpose of these attacks at this stage appears to have been to disrupt computers, rendering them unusable, or crashing exile media websites, rather than for the purpose of monitoring user activity.[425] However more recently, the purpose of malware attacks seem to have been to gain access to confidential information (See above and Chapter 4.4 on Surveillance).

Existing Cyber Security Management and Policy in Myanmar

As the ICT sector grows in Myanmar, and more services are introduced online, such as e-banking, maintaining the availability of services, integrity of systems and protection of

[420] See Infosecurity, "Massive DDoS Attack Knocks Burma Offline" (5 November 2010).
[421] Shawn W. Crispin, "Burmese Exile News Site Endures Hacking, DDoS Attacks" *Committee to Protect Journalists (CPJ)* (2 May 2011).
[422] Bill O'Toole, "Email Hacking Exposes Cybercrime in Myanmar" *The Myanmar Times* (20 February 2013).
[423] Softpedia, "1,000 Myanmar Websites Hacked by Blink Hacker Group" (3 January 2013) and Blink Hackers Group.
[424] A denial of service attack involves flooding a network with information, which overwhelms a website or services server used for hosting. This can involve a single attacker, or a group of compromised computers (bot-net) that flood the network (called a distributed denial of service attack).
[425] Rehmonnya.org "'I Need Help' Email Virus Attacks Burmese Exile Groups" (4 October 2008).

information against attacks will become a central issue to the Government of Myanmar's internet governance policy. However, there is currently no legal framework in Myanmar that clearly defines what constitutes Personally Identifiable Information (PII) or stipulates any requirements around the collection, management, or transfer of personal data for companies. Hacking is criminalised under article 34 of the Electronic Transactions Law (No 5/2004).[426] A cyber-security/cyber-crime law is rumoured to be in development by either the Ministry of Information and Communication Technology or the Ministry of Home Affairs, both with likely support from the Myanmar Computer Federation (MCF). A specific timeline for the law's development is unclear. In 2014 it was reported that the Government was seeking support and knowledge sharing opportunities from private companies in the cybersecurity space, such as Microsoft.[427]

One of the high priority items under the 2011–2015 ICT Master Plan's Infrastructure component is the establishment of a "Cyber Security Centre"[428], including the creation of a *Cyber Information Act* and Information Security Committee to select the specific technology (hardware and software) that would be used by the Cyber Security Centre. The follow up report to the 2005-2010 ICT Master Plan states the intention to build a Cybersecurity Protection Agency to protect Myanmar's critical information and infrastructure[429], whose role is to enhance Internet security and creating a safe Internet environment. It states the strategic objectives of this agency are to *"Prevent cyber-attacks against Myanmar's critical infrastructures; Reduce national vulnerability to cyber-attacks; Minimise damage and recovery time from cyber-attacks that do occur".* In addition, the agency would protect citizen's personal information, provide guidance and training for Internet and information security, protect critical infrastructure by analysing and evaluating weaknesses in facilities, strengthening security for electronic government services and protection of public information. In 2015, MCIT published a draft ICT Master Plan for public consultation.[430] It outlined plans to create and publish a national cyber security policy by 2016, but did not repeat the specifics outlined in the 2011 follow up report.

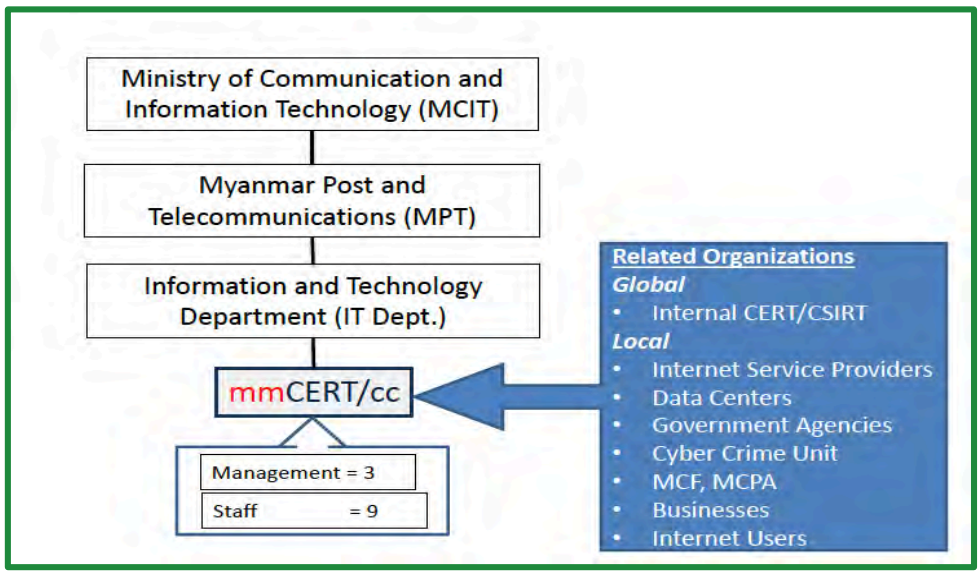
[426] Myanmar *Electronic Transactions Law*.
427 Htun Htun Minn, "Microsoft Tapped To Assist Myanmar Develop Cyber Security Measures" *Myanmar Business Today* (24 June 2014).
[428] See, Ministry of Communications and Information Technology, "The Follow-Up Project of the Establishment of an ICT Master Plan: Final Report" (2011), pages 89-94.
[429] Ibid, Section 3.6.1.6.
[430] See MCIT, "Draft Telecommunications Masterplan" (7 August 2015) and MCRB, "Comments on the draft Myanmar Telecommunications Master Plan" (30 July 2015).

The Role of the Myanmar Computer Emergency Response Team (MMCERT).

Cybersecurity is currently managed by a single organisation called the Myanmar Computer Emergency Response Team (MMCERT), under the Ministry of Communications and Information Technology (MCIT). It is unclear how MMCERT will operate under the planned restructure outlined in the Telecoms Master Plan, where it is not mentioned at all.

Currently, MMCERT exists to disseminate advice and best practices regarding cyber security, provide technical assistance through workshops and seminars, and to cooperate with law enforcement officials on cyber-crime or security issues. MMCERT maintains a ticketing system for case management of cyber security issues. Users can submit a case report via email. [431] MMCERT posts updates regarding known software security vulnerabilities on their home page (e.g. WordPress, Microsoft, Oracle, etc).

Figure 5: Relationship between MMCERT and MCIT



Source: *International Telecommunications Union (ITU)*

MMCERT is an operational member of the Asia Pacific Computer Emergency Response Team (APCERT).[432] The purpose of APCERT is to provide coordination among regional computer emergency response teams, develop responses to large-scale security threats and facilitate research and development among APCERT members. MMCERT is also a member of International Multilateral Partnership Against Cyber Threats (IMPACT).[433]

Outside of these affiliations, stakeholders in Myanmar's ICT business community note that MMCERT lacks the "funding, sponsorship, and support" needed to adequately address cyber-security threats in Myanmar's rapidly evolving ICT sector. Some private

[431] MMCERT, "Incident Report" (last accessed September 2015).
[432] APCERT defines an operational member as a, "*CSIRT [Computer Security Incident Response Team]/ [Computer Emergency Response Team] CERT in the Asia Pacific region, which performs the function of CSIRT/CERT on a full time basis as a leading or national CSIRT/CERT within its own economy.*" See: Asia-Pacific Computer Emergency Response Team, "Operational Framework" (2009).
[433] IMPACT is a partner of the United Nation's International Telecommunication Union (ITU). The IMPACT/ITU partnership is primarily based on implementing the ITU's Global Cyber Security Agenda (GCA).

stakeholders view Myanmar's lack of existing infrastructure as an opportunity, allowing Myanmar to "leapfrog" legacy technology and implement cutting edge infrastructure. For many Myanmar businesses, a desire to deploy modern technology has overshadowed the importance of cyber-security and data protection policies.

B. Field Assessment Findings

See also field research findings in Chapter 4.3 on Privacy, which are also relevant for cybersecurity issues**.**

Cyber Security
Human Rights Implicated: Right to privacy
▪ **Low awareness of cybersecurity risk by business**: The majority of companies did not have policies in place to test their systems against threats. Only one company interviewed carried out ongoing penetration and vulnerability tests to mitigate risk. ▪ **Lack of awareness of cybersecurity risks among users**: Users on social media were observed sharing sensitive personal data including bank statements and checks for donations. Users also reported being unaware of how to configure privacy settings in their social media accounts. ▪ **Use of pirated applications in mobile shops:** Many users also download pirated applications on their mobile phones at phone shops, unaware of the specific application permissions the software required or that an application could contain malware. ▪ **Lack of identified Personally Identifiable Information**: An independent cyber-security professional noted that companies in Myanmar have not defined what constitutes Personally Identifiable Information (PII) (information that can used to "distinguish or trace" an individual's identity), or who has the ability to access this information internally.[434]

C. Cybersecurity: Recommendations for ICT Companies

- **Raise awareness of users about protecting themselves online**: Users in Myanmar generally have a very low level of awareness around cybersecurity, including the use of passwords or keeping personal information safe. Both government and business should address the need to raise cybersecurity awareness among users.
- **Employ the maximum security for user communication:** At a minimum, companies that provide online communications and transactions, such as email, social networking and shopping, should use industry standard encryption such as 'https', which encrypts traffic between a web browser and the server of the service being accessed, strengthening the privacy of communications and transactions online.[435]
- **Be prepared for a cyber-attack by developing a response plan**. As noted above, there are currently no laws on cybersecurity, data protection and little in the way of support from overstretched government resources in terms of supporting smaller or newer businesses in developing their cybersecurity approach. This could be an important area of collective action by the larger multinational ICT companies to

[434] National Institute of Standards and Technology, "Guide to Protecting the Confidentiality of Personally Identifiable Information (PII)" (2010).
[435] Mike Shema, "*Web Security: Why You Should Always Use HTTPS*" *Mashable* (31 May 2011).

support local industry associations or other initiatives to improve protection among local businesses. It should be possible to detect an attack quickly and respond to secure data and minimise damage. If companies do not do all they can to keep services available, maintain the integrity of their systems, and protect the confidentiality of user data they could suffer a loss of trust from users, impose costs and liabilities on users and potentially on themselves.

- **Clearly communicate to customers or users what data is being collected and why**: Field research findings demonstrate that few companies in Myanmar have privacy policies or communicate their policies to users (See Chapter 4.3 on Privacy).
- **Conduct on-going vulnerability assessments and penetration tests**: It is critical that businesses are aware of potential vulnerabilities in their internal systems. This involves ensuring that all "information assets" (servers, applications, databases, paper files) are protected from unauthorised access. Using licensed software means that companies will have access to the latest available version from the developer and fixes for security vulnerabilities through software updates.
- **Particularly protect vulnerable users:** Civil society groups are often the target of cyberattacks, either to disrupt the spread of information or gain confidential information, such as journalist sources, from email accounts and servers. (See Chapter 4.8 on Groups at Risk). Companies could open a channel of communication with Myanmar's civil society groups so they can quickly be notified if such events occur. In the event of a data breach, companies should notify users if there has been a data breach or if they suspect a state-sponsored attack has taken place on their email accounts.[436] This enables users to take action to secure information or warn others. In 2013, a number of journalists covering issues in Myanmar received these warnings.[437]

D. Relevant International Standards on Cyber Security

Relevant International Standards:

- Council of Europe, Convention on Cybercrime (Budapest Convention)

Relevant Guidance:

- Council on Cyber Security, "The Critical Security Controls for Effective Cyber Security Defense, version 5.1"
- Australian Department of Defense, "Strategies to Mitigate Cyber Intrusion"
- Council of Europe, "Global Alliance on Cyber Crime – GLACY"

[436] Google Online Security Blog, "Security Warnings for Suspected State-Sponsored Attacks" (5 June 2012).
[437] John Ribeiro, "Google Warns Reporters Covering Myanmar of 'State-Sponsored' Attacks on Gmail Accounts" (11 February 2013).

Chapter 4.6
Labour

4
4.6

Chapter 4.6
Labour

In this Chapter:

A. Context

Worker rights in Myanmar have experienced numerous challenges. For 50 years, independent trade unions and employer organisations were prohibited; laws covering labour protection were antiquated and/or restrictive; forced labour of civilians by the military and civil authorities was common; and child labour is still an ongoing problem. There have however been positive developments since the 2011 reform process began.

The 2008 Constitution includes protection from discrimination and freedom of association, though these constitutional provisions contain some significant gaps in protecting workers rights. Article 358 of the Constitution prohibits slavery and human trafficking, but Article 359 provides for "*hard labour*" as part of a criminal sentence. The rights to peaceful assembly and freedom of association are also provided for, but another part of the Constitution subjects the exercise of these rights to a wide qualifier that the exercise of the rights cannot be contrary to laws on *inter alia* "*community peace and tranquillity*". Article 31 of the Constitution aims to reduce unemployment. Under Article 349(b), citizens have the enforceable right to equal opportunity in occupation.[438]

An estimated 70% of the population is engaged in agriculture or related activities; 23% in services, and 7% in industry.[439] Low-paid and insecure jobs (often only on a daily basis) characterise the employment situation. The 2014 Census results indicate an

[438] Legal Analysis of the 2008 Constitution, Appendix 1, commissioned by IHRB.
[439] Labour Background Paper commissioned for IHRB, p 2 (on file with IHRB).

unemployment rate of 4% for workers age 10 and over; 3.9% for over 15s; and 4% for ages 15-64. The Census reports a labour force participation rate of 57% for those aged 10 and over; 64.4% of those 15 and over; and 67% of those aged 15 – 64.[440] Underemployment in Myanmar was 37% in 2010, affecting rural and urban areas, poor and non-poor, male and female alike, and young people in particular.[441] To improve the quality of statistical data on labour, the Ministry of Labour, Employment and Social Security, with International Labour Organisation (ILO) support, is undertaking a comprehensive national labour force survey,[442] with results expected in late 2015. The lack of reliable statistics and accurate data hold true for the ICT industry workforce.

According to the General Secretary of the Myanmar Computer Federation, Myanmar has an estimated 1,600 software engineers, 1,000 network engineers, including those working in the telecom companies and about 1,000 service technicians, including handset repair technicians. No statistics on fibre installation or tower construction workers are available. It is also estimated that by 2025, Myanmar will have 25,000 engineers. Currently, there are 26 Computer Universities in Myanmar. There is no existing data on the employment rate of ICT university graduates.

The development of the ICT industry has led to a dramatic increase in jobs in the sector. According to a survey conducted by work.com.mm, an online job search company, during the month of April 2015, the highest number of job announcements was in the field of engineering, followed by the software and IT sector. [443] There is however a mismatch between demand and the quality of supply, a consequence of poor quality ICT education. There are many ICT graduates, but few who are qualified, and those there are often leave Myanmar for better work opportunities abroad.

As to the international telecom operators, Ooredoo currently has around 1,000 employees of whom 87% are Myanmar nationals (41% male/59% female). Ooredoo has committed to the Government to employ 99% Myanmar nationals within 5 years. Telenor Myanmar currently has 478 employees (64% male/36% female) of whom 80% are Myanmar nationals. There are no statistics on the number of people working as SIM card and phone vendors at points of sale, but operators have set targets: Ooredoo promises 240,000 SIM card sale points and 720,000 top-up locations; Telenor aims for 70,000 SIM card sale points and 95,000 top-up locations.

ILO Fundamental Principles and Rights at Work: Freedom of Association and the Right to Collective Bargaining in Myanmar

For the first time in 50 years, the 2008 Constitution and new labour laws provide for independent trade union activity, though some gaps in protecting freedom of association remain. The 2011 *Labour Organisation Law* permits the exercise of freedom of association and the 2012 *Settlement of Labour Dispute Law* provides for disputes resolution institutions and mechanisms. Parliament amended the latter law in October 2014 providing for *inter alia* increased fines for employers who break this law, but rejected

[440] The Republic of the Union of Myanmar, "2014 Myanmar Population and Housing Census, Census Report Volume 2-A" (May 2015).
[441] Underemployment refers to people who worked or had a job during the reference week but were willing and available to work more. ILO, "Underemployment Statistics" (last accessed August 2015).
[442] ILO, "Myanmar sign agreement on National Labour Force Summary", (14 November 2013). The survey is intended to inform national labour policy and will examine youth employment, child labour, forced labour, and social security.
[443] Internet Journal, "The top job in the field of telecommunications services" (15 May 2015) (Burmese).

the President's proposal which provided for imprisonment of such employers.[444] In May 2015, the ILO reported that over 1660 independent trade unions have been registered, mostly at the enterprise level.[445] While these are predominantly based within the apparel, other manufacturing or farming sectors, at least one of the international telecommunications operators, Telenor, has a global framework agreement with the union representing service sector workers around the world. The agreement provides a platform and framework for dialogue between UNI Global and Telenor on fundamental labour rights that can also cover a dialogue on working conditions in Myanmar.[446]

On a national scale, there is an opportunity to build from scratch the sort of 'development' model of industrial relations the country needs. However, the current laws relating to freedom of association and collective bargaining mentioned above promote fragmentation of industrial relations by making it difficult for unions to establish themselves beyond the enterprise level. A lack of understanding, or in some cases entrenched attitudes, might see the new rights-based industrial relations framework drift towards a conflict model. This risk has been increased by the perceptions created by several high profile labour disputes and the weaknesses in the law and its implementation, which mean that, in practice, employers can discriminate against workers who seek to exercise their rights in accordance with the new laws, including by dismissing them from their jobs.

Early 2015 saw a number of strikes and protests in Yangon by garment factory workers calling for higher wages and better working conditions. Although some disputes were resolved by employer-worker meetings, others were not, leading to protest demonstrations and arrests of workers.[447] An ILO official noted in August 2014 that factory owners appear to be dismissing employees because of their union activities and recommended that the Government outlaw this practice.[448] The ILO has recommended a number of amendments to the new laws on freedom of association to improve their functioning, including an obligation on parties to engage in collective bargaining in good faith, and to strengthen the enforceability of decisions of the labour arbitration bodies.

[444] Unofficial translation of The Republic of the Union of Myanmar, Board of Information, Issue No (5/2014), October 14, 2014, announcing the Draft Bill which amends the Settlement of Labour Dispute Law, on file with IHRB/MCRB.
[445] Mizzima "Unions have hit a glass ceiling" (10 March 2015).
[446] Telenor, "Telenor renews global agreement with UNI Global Union" (May 2015).
[447] Myanmar Times "Time for government to step up on labour disputes" (17 March 2015).
[448] DVB, "Burma's Industrial Relations at a Crossroads" (30 August 2014).

ILO Fundamental Principles and Rights at Work: Discrimination in Myanmar

Article 348 of the 2008 Constitution guarantees that discrimination by the Union against any citizen is prohibited on grounds of race, birth, religion, official position, status, culture, sex and wealth. However, the internationally recognised grounds of discrimination based on colour, language, political or other opinion and national origin are not prohibited by the Constitution, leaving significant gaps in protection against discrimination. Labour leaders, religious and ethnic minorities, women and children, people living with disabilities and LGBT people (as discussed in further detail in Chapter 4.8 on Groups at Risk) all face discrimination in hiring and in the workplace.

ILO Fundamental Principles and Rights at Work: Forced Labour in Myanmar

A major concern in Myanmar has been the widespread and systematic use of forced labour of civilians by the *tatmadaw* (the Myanmar army) and the civil administration for several decades, despite the fact that the Government had ratified *ILO Forced Labour Convention (No. 29)* in 1955. The ILO first established an office in Myanmar during 2002 after the Government and the ILO reached an "*understanding*" and the appointment of an ILO Liaison Officer. The Understanding provided that the Liaison Officer would conduct activities aimed at the elimination of forced labour in the country. The Understanding remains in force and in 2007 the ILO and the Government agreed a Supplementary Understanding. The Supplementary Understanding established a complaints mechanism to allow victims of forced labour to seek redress/remedies from the authorities.[449] Since the reform process began in 2011, many observers, including the ILO, have welcomed the decrease in forced labour, but noted that the practice is still continuing in some areas.[450] President U Thein Sein made a public commitment to end forced labour by 2015.

Although there is now less risk to communities and companies of forced labour being used by the military in relation to projects, such as road construction, there is a need to remain vigilant, as it was a common practice for several decades, and local Government and other authority figures still sometimes resort to it. The ILO noted that while there are currently relatively few complaints of forced labour in the private sector, this may be because in Myanmar forced labour is generally perceived to be associated with the Government[451].

ILO Fundamental Principles and Rights at Work: Child Labour in Myanmar

Child labour is widespread throughout Myanmar, including as tea shop or restaurant attendants, street vendors, manual labour, waste collectors or beggars, in food processing and light manufacturing, and on farms in rural areas. The risk of child labour to companies operating in Myanmar is high, as they are working in a wide variety of industry sectors. Moreover, ascertaining someone's age in Myanmar is not always straightforward. Birth registration in urban areas was reported at 94%, but in rural areas the rate was only 64%.[452] Many people, especially under-18s and ethnic minorities, do not have any form of official identification which indicates their date of birth.

---

[449] See: ILO, "ILO in Myanmar" (last accessed August 2015).
[450] ILO Committee on the Application of Standards, "Extract from Record of Proceedings" (June 2012), para18
[451] ILO, "Update on the operation of the complaint mechanism in Myanmar", *Report of the ILO Liaison Officer to ILO Governing Body, 319th Session, Geneva* (16-31 October 2013), GB.319/INS/INF/2. Please note that complaints include underage military recruitment.
[452] UNICEF, "Situation Analysis of Children in Myanmar 2012" (2012).

An August 2014 report by one telecoms operator noted that on-site inspections of its supply chain found cases of underage labour (15 – 17 years old) and child labour (under 15 years old), including on tower construction sites.[453] In May 2015 the same company reported they had uncovered additional cases of child and underage labour in its supply chain, as they continued their work to eradicate all such cases in tower construction sites. The Government's ratification of *ILO Convention No 182 on the Worst Forms of Child Labour* in December 2013[454] is part of the Ministry of Labour's reported aim to eradicate the worst forms of child labour by 2015. Parliament approved the ratification of the convention in July 2014, with full implementation pledged by the Government in December 2014 although this has yet to take place.[455]

Overview of the Revision of Myanmar Labour Laws

In addition to the laws on freedom of association and collective bargaining noted above, new labour laws passed by Parliament since the 2011 elections include the 2013 *Minimum Wage Act,* the 2012 *Social Security Law*, and the 2013 *Employment and Skills Development Law*. Other laws are believed to be in draft form or in the process of being drafted, including a *Shops and Enterprises Act*, an *Occupational Health and Safety Act,* a *Factories Act Amendment Bill* and a *Foreign Workers Act.* The ILO is currently working with the Government to come up with an overall legal and policy framework on labour, with the aim of drafting one comprehensive labour code after 2015 that would consolidate these laws and draft laws into a coherent code or framework.[456] Given the rapid enactment of labour laws, it is likely that there will be overlap and contradiction within the laws, at least until the more comprehensive labour code is in place.

Working hours are generally very long but with new labour laws in place, there is a focus on reducing hours. The 2012 *Minimum Wage Law* provides for a minimum wage to be set. This finally took place in August 2015 when the rate was set at 3,600 MMK per day.[457] The *Minimum Wage Law* requires that salaried workers should have one day off per week with pay, and the payment of over-time if a salaried worker works on the day of leave (Article 16d). Protections for daily wage workers are predictably less. However, if a worker in a daily wage job works less than the set hours per day because the employer requires fewer hours, the worker should still receive the full wage for the day (Article 16(e)). The law covers part-time work, hourly jobs and piecework (Article 16c) and provides that both men and women should receive the minimum wage without discrimination (Article 16f). The *Minimum Wage Law* also provides for penalties if the employer fails to pay the minimum wage.[458]

The 2012 *Social Security Law* provides for a health and social care insurance system; a family assistance insurance system; invalidity benefit, superannuation benefit and survivors' benefit insurance system; and an unemployment benefit insurance system from

[453] Telenor Myanmar, "Business Sustainability Update" (19 August 2014). Children were immediately removed from the sites. The company's policy states that no one under 15 will be employed and that workers must be at least 18 years of age to work on tower construction sites, as the company considers the work to be potentially hazardous. It also works to educate and train local suppliers and the community on its child labour policies. See also Myanmar Times, "Telenor works to address its child labour troubles", (22 May 2015).
[454] Eleven Media, "Myanmar Vows To Root out Child Labour By 2015" (4 May 2014).
[455] The Irrawaddy, "Govt to Start Child Labor Elimination Policy in December" (18 July 2014).
[456] ILO is expecting to put in place a full Decent Work country programme in 2016.
[457] Myanmar Times, "Minimum wage set at K3600" (19 August 2015).
[458] Myanmar Ministry of Labour, Employment and Social Security, *2012 Minimum Wage Law*.

a social security fund, which both employers and workers pay into. The Law revokes the 1954 *Social Security Act*,[459] and came into effect on 1 April 2014.[460] The *Social Security Rules* (Notification No. 41/2014) are also in place.[461] However, as of January 2015 only 1.5% of the population was registered in the social security system, according to a Ministry of Labour official.[462] It appears that companies with two or more employees, including those in the ICT sector, are required to pay social security.[463]

The 2013 *Employment and Skills Development Law* provides for skills training and a fund into which employers pay. The law also provides for the establishment of an employment and labour exchange office by the Ministry of Labour, Employment and Social Security. Significantly, written employment agreements between employer and employee will now be required under Chapter 3 of the law. The law went into effect on 30 November 2013 and revoked the 1950 *Employment and Training Act*.[464]

The 1951 *Leave and Holiday Act* was amended in July 2014 and provides for leave, holiday, maternity leave and covers daily wage, temporary and permanent workers.[465] The forthcoming *Occupational Health and Safety Act* is expected to be passed by Parliament by September 2015.

Chapter II (Article 3) of the *Settlement of Labour Dispute Law* requires an employer with more than 30 workers to form a Workplace Coordinating Committee (2 representatives of workers, 2 representatives of employer) whether or not there is a labour organisation (e.g. union) in the enterprise.

Awareness and Enforcement of Labour Rights in Myanmar

There is an overall lack of awareness by workers and employers of these new legal rights and safeguards, including lack of understanding of the concept of a minimum wage. The ILO, trade unions, and other labour activists are helping to inform both workers and employers about the new labour laws and poorly understood concepts such as collective bargaining and a minimum wage. So far enforcement of the new laws is piecemeal, and full-scale implementation will be a long-term process. Although the Factories and General Labour Law Inspection Department (FGLLID) is the main Government agency responsible for occupational safety and health, a number of other agencies in other ministries are responsible for specific areas or sectors related to safety and health at work and/or public safety and health in general. These include the Ministry of Mines, Ministry of Industry (boilers and electrical equipment), Ministry of Construction, Ministry of Agriculture and Ministry of Health etc.[466] The Government recognises the need for a greater number of trained labour inspectors for worksites and is reportedly taking steps to increase the number of qualified inspectors.

---

[459] *The Social Security Law*, 2012, on file with IHRB.
[460] New Light of Myanmar, "State is also exerting efforts to ensure fair protections without affecting the interest of both workers and employers" (1 May 2014).
[461] Myanmar Garment Manufacturers Association "Labour Laws and Regulations" (accessed August 2015).
[462] Mizzima "Social Security Sign-up slow in coming"(5 January 2015).
[463] This excludes except for government departments, international organisations, seasonal farming and fishing, non profit organisations, establishments operating less than three months, family and domestic businesses. *Social Security Law*, August 2012, Section 11, a) and b) and Section 12, b), on file with IHRB/MCRB.
[464] *Employment and Skill Development Law* (2013), unofficial translation on file with IHRB.
[465] Myanmar Garment Manufacturers Association "Labour Laws and Regulations" (last accessed August 2015).
[466] Labour Briefing paper commissioned by IHRB, August 2013, on file with IHRB.

B. Field Research Findings

The following findings concerning respect for the rights of workers, while not universal, were found to be widespread in the field. Examples of good practice observed are included at the end of the chapter.

ILO Fundamental Principles and Rights at Work:
Freedom of Association & the Right to Collective Bargaining

Human Rights Implicated: Right to peaceful assembly; Right to freedom of association and collective bargaining

Field Assessment Findings

- There was a general **lack of worker-management engagement** in most companies across the ICT value chain, and only a few companies provided grievance mechanisms through which workers could raise complaints regarding their jobs and seek a resolution.
- **Unskilled workers tend to be relieved to secure a job at all** because the supply of workers exceeds work available. This leads to a tendency for workers to **refrain from raising workplace and employment related complaints**, such as unpaid or inadequate wages, poor health and safety standards, or barriers to unionising.
- **At fibre factories, workers were unaware of their basic association and collective bargaining rights,** or the requirements to form a union, such as that there must be a minimum of 30 members**.** They did not feel the company would allow it even if it was permitted under national law. They were also concerned that joining a political party could also affect their jobs.
  - Workers were **able to raise complaints at meetings or anonymously through a letter box system**, but issues previously raised, such as deductions from daily wages and bonuses had **failed to be addressed**.

ILO Fundamental Principles and Rights at Work:
Non-Discrimination

Human Rights Implicated: Right to non-discrimination; Right to work; Right to just and favourable conditions of work

Field Assessment Findings

- It was very unusual for **any women to work on tower construction**.
  - This was often justified on the grounds that it unsafe for them due to night work and distances between the site and their village/ accommodation.
  - Where women were able to work on tower construction sites, they were only allowed to do certain manual tasks, such as backfilling or moving materials.
- **Racial and religious tensions were observed in some areas, mainly where communities identified the company or its workers as Muslim** This followed intercommunal violence in other parts of the country**:**
  - Researchers heard of several incidents in which subcontractors of a company from a majority Muslim country were disturbed by communities protesting the company's presence.
  - Workers were denied accommodation due to working for that company;
  - Communities threw stones at cars carrying workers of companies that were perceived to be owned by Muslims.

ILO Fundamental Principles and Rights at Work: Forced Labour and Child Labour

Human Rights Implicated: Right to freedom from forced labour and servitude; Right to freedom from child labour; Right to an adequate standard of living; Right to education

Field Assessment Findings

- Researchers heard of **several cases where workers were brought on to dig fibre cable trenches due to a debt owed to the group leader**. This often arose where workers asked for advance payments during the rainy season in order to make ends meet until the next crop yields. As such, workers were often in positions of **debt bondage**, reporting that where they expressed a wish to quit or move to another job the creditor threatened to increase interest rates.
  - This impact was heightened where workers were also required to purchase food, water and other supplies from labour leaders, often at inflated prices and on a credit-based system.
- Occasional practices of reviewing identification to verify workers' age were reported, but many more instances of lack of identification cards or documents were described to researchers, indicating a **general lack of basic measures to prevent underage workers in fibre cable digging in particular**.
- Fibre cable line workers often had to travel long distances from their homes in order to take up work. They sometimes brought their children with them as they could not afford child care or because it was difficult to reliably arrange due to moving from site to site regularly. As such, **children were regularly left with someone connected to the works in the worker camps during the 10 hour shift periods**.

Employment Status

Human Rights Implicated: Right to just and favourable conditions of work; Right to equal payment for equal work

Field Assessment Findings

- Across the ICT value chain **employment contracts were not being used** in the majority of observed cases**,** with the limited exception of direct, permanent employees of a tower company.[467]
  - Consequently, **wage slips** itemising pay and deductions were not being provided.
- It was reported that manual labourers and construction workers regularly secured jobs through relatives/connections. Wages were already negotiated and contracts were not given, as workers will "take what they are given".

[467] The research team was not permitted to meet the staff of the telecoms operators so this does not necessarily apply to those employers.

Working Hours, Wages and Benefits

Human Rights Implicated: Right to just and favourable conditions of work; Right to an adequate standard of living

Field Assessment Findings

- **Daily wage workers** typically worked every day possible to maximise income while work was available, thereby exceeding legal working time limits
- **Awareness of rights to wages and benefits varied considerably**. Many workers admitted to a **very low level of understanding of their rights** vis-à-vis employers or the Government. There was also little to no information regarding labour rights or working conditions shared proactively by most companies with their workers, which will be important as a number of new labour laws such as the *Minimum Wage Law* have recently come into force.
- **For tower construction:**
  - It was regularly reported to researchers that **workers did not receive any rest days until after the completion of a site**, i.e. usually a 1-1.5 month build period.
  - **Working hours** were often 7 or 8 a.m. until 5 or 6 p.m. with a (usually 30-60 minute) lunch break. A second night shift was occasionally reported of 7 p.m. to 11 p.m.
  - **Wage rates varied** depending whether workers were directly employed by tower companies, labour sub-contractors, or brought on for peak periods (such as on foundation sections) as day labourers from nearby villages.
    - Worker daily wages were reported anywhere between 5,000 MMK per day up to 15,000 MMK (30,000 MMK if able to work a double shift)
    - Overtime was not usually paid. Where it was reported as a practice, for example where workers worked beyond 11 p.m., the rate given was not specified.
- **For fibre line digging:**
  - **Working hours** were commonly cited as 6 or 7 a.m. to 6 or 7 p.m. by managers, but workers often reported that they were often pressured to continue until target distances were dug regardless of the hours worked.
  - **Workers were not given set rest days** as they were not paid until their target distance had been dug, which was dependent on soil conditions and the number of workers grouped together.
  - **Wages often did not amount to levels sufficient to cover basic needs:**
    - Workers were paid according to distance dug, with no reflection of soil conditions or geography where it takes more time and effort to achieve the same distances. In terrain where distances were harder to achieve, workers regularly struggled to earn enough to feed themselves or families.
    - **Sick pay was not provided**. As such, workers continued to work 12 hour days of hard labour even when ill in order to ensure their incomes.
- **For fibre cable factories:**
  - Working hours:
    - Working hours lasted around 8 hours per day.
    - Overtime was only paid after 8 years of continuous work.
  - Wages:
    - The basic daily wage rate was 2,200 MMK ($2.00), but workers reported not receiving salary increases or promotion despite 4 or 5 years continuous service.

  - Bonuses were reportedly provided for regular attendance.
- Leave:
  - Workers received one and a half days off per week.
  - Workers were able to take public holidays off with pay.
  - Workers did not receive paid sick leave or company-provided insurance.
  - Workers received 10 days unpaid annual leave.
  - Female workers were entitled to three months paid maternity leave at the basic salary band.

Working Conditions and Provision of Facilities to Workers

Human Rights Implicated: Right to an adequate standard of living; Right to just and favourable conditions of work; Right to non-discrimination

Field Assessment Findings

- **Observed working conditions for fibre cable digging were particularly harsh:**
  - **Workers had to dig long distances of trenches manually**, without any mechanical digging or drilling equipment, even in mountainous and rocky areas.
  - As noted above, **12 hour work days** were common practice.
  - **Workers were expected to dig set distances each day,** ranging from 2 – 10 metres each day per worker.
  - **If a worker was injured, they had to repay any medical expenses** covered by their company.
  - **Language barriers** were a commonly reported problem between managers and workers. Researchers heard that workers were often unsure whether any complaints or issues they raised were properly reported to the managers responsible.
- **Little to no facilities or equipment were provided to fibre cable diggers:**
  - **Workers were not provided with any equipment** such as shovels and pick axes and had to pay for their own tools or had the costs deducted from their salaries.
  - **Workers were not provided drinking water** and had to source their own, for example requesting from surrounding residents or boiling ground water.
  - **Workers had to find or build their own accommodation with their own money**, despite often being transported long distances from their homes for long periods of time in order to continue working on the lines. This **usually consisted of make-shift tents from tarpaulins and sticks**. Camp areas were commonly in nearby fields or off the side of the road and did not have any running water, power or adequate sanitation facilities.
  - Workers had to **pay for all food and supplies while on the job**, despite relocating far from home for long periods of time to undertake the work.
    - Workers were **commonly required to buy food through the wife of the group labour leader**, and several reports were received of **charging workers prices far above market value** for their food supplies.
    - Workers often had to **similarly pay for other supplies:** candles, blankets, mattresses, buckets of water to cook or shower with, and wood for cooking.
- **Some fibre factory workers were provided with accommodation** in permanent structures that were heated and had running water and electricity.
  - Workers' families were allowed to stay with them.
  - Rooms were reportedly 10 square feet, though researchers were unable to visit them due to time constraints.

- Workers were provided three meals per day, consisting of unlimited rice and up to two cuts of meat.

Health, Safety & Environment (HSE)

Human Rights Implicated: Right to the highest attainable standard of physical and mental health; Right to life, liberty and security of the person

Field Assessment Findings

- Workers of subcontractors were commonly not informed about which tower construction company or telecoms operator the tower was being built for, which implies that the operator's and their 1st tier subcontractor's **health and safety and other operational standards may not have been transmitted to the site level**.
- **Workplace attention to health and safety varied greatly** amongst the tower and fibre sites visited by researchers.
- Field teams regularly witnessed tower construction workers and fibre trench workers **without personal protective equipment (PPE)**, for example:
  - Not fastening **safety harnesses** when climbing the towers
  - No **gloves**, e.g. while digging fibre cable trenches
  - **Canvas shoes** rather than hard toed shoes
  - No **hard hats**
- **Even where workers had PPE to hand:**
  - Researchers observed a number of occasions where **workers asked if they "*actually needed to wear it*"** or companies reporting workers not wearing it due to discomfort, such as not wearing safety suits in hotter weather, indicating lack of enforcement of PPE use by all workers while on site.
  - It was common for workers to have to **buy or replace their own PPE, or compensate the value if they damaged it while working**.
- **Failure to ensure that emergency first aid kits were available at tower sites** was also a common occurrence**.**
  - Where companies did provide first aid kits or fire extinguishers, workers reported they **did not know how to use them** in cases of emergencies and had not been provided any training.
- **For fibre factories:**
  - PPE in the form of cotton gloves was provided.
  - Workers received training on how to work machines and use the fire extinguisher.

Conflict Areas

Human Rights Implicated: Right to life, liberty and security of the person; Right to take part in the conduct of public affairs; Right to information

Field Assessment Findings

- There were some cases in which companies attempted to negotiate access to areas to lay fibre cables with non-state armed groups (NSAGs). **In some cases a fee was paid for this access.**
- Researchers received reports of cases of operational delays, where local groups, including armed groups, **blocked access to sites, due to lack of consultation at the site level.** While some consultation with local leaders may have been undertaken, this may not have been communicated to or accepted by all stakeholders.

- Researchers observed **fire-arms being carried by NSAGs** present during roll-out in ceasefire areas. While researchers neither observed not heard reports of shots being fired, the presence of fire-arms is a risk.
- Researchers also received reports from workers that they were aware that landmines **may have been sowed in the past, with land mines around infrastructure in conflict areas**. This led workers to avoid walking through certain areas. The measures companies took to protect their workers in such circumstances were unclear.

Business Relationships

Human Rights Implicated: Right to just and favourable conditions of work

Field Assessment Findings

- **Tower company acknowledgement and action concerning their responsibility for the safety of workers was uneven.**
  - Some tower companies indicated worker safety was **the responsibility of their subcontractors alone**. They did not provide any safety guidelines or training to subcontractor managers or workers, did not regularly monitor site safety or track incidents.
  - **Others undertook subcontractor skills-based and safety training and regular site monitoring to ensure safety standards** were upheld and practices corrected.
  - Of those tower companies who had systems in place for incident reporting and raising issues to more senior levels of the company depending on the severity of the incident, it was reported that **labour subcontractors may fear reporting incidents for fear of reprisal or lost business**.
- **Choosing to operate without contracts between tower companies and their subcontractors was a common occurrence**. This indicates the more rigorous control of working conditions by telecoms operators is not consistently carried through to business partners by contractual conditions committing sub-contractors to meeting business partners' standards.

Myanmar Good Practice Examples:

- Some subcontractors ensured PPE was provided to their workers and used, provided emergency first aid kits and fire extinguishers, and paid workers' medical bills where incidents arose, despite not receiving safety guidelines or training from tower companies or telecoms operators.
- A small number of fibre cable digging companies provided workers with digging equipment, PPE and tents and supplies for accommodation without charge.
- One company has reported it has a zero tolerance policy for employment discrimination, and child and forced labour, stating health and safety and a living wage are key considerations.[468]
- One company has reported that its Myanmar operations are governed by a Code of Conduct and Code of Business Ethics, covering land, labour, health and safety, the environment, anti-discrimination, and privacy/freedom of expression. It conducted a

[468] See further: Apollo Towers Myanmar, "Response by Apollo Towers: Myanmar Foreign Investment Tracking Project", *Business & Human Rights Resource Centre* (last accessed September 2015).

human rights impact assessment in 2013, which identified key risks that will be reflected in its management systems.[469]

- One company has reported that it has no manufacturing facilities but does have a small sales force in Myanmar. It applies its global policies on labour rights, health and safety, child and forced labour, living wage, anti-discrimination, and the environment.[470]

C. Labour: Recommendations for ICT Companies

Using International Standards

- **Use international standards as a basis for relationships with workers:** Given the large number of labour laws being enacted, it is likely that there will be overlap and contradiction between and within the laws. As noted above, the ILO is working with the Government to develop one harmonised, overarching labour code that is expected to be better aligned with ILO standards. Until such time, using international standards rather than Myanmar law is a better basis for developing policies and practices that respect the human rights of workers (see Part D).

Recommendations on Workplace Issues

- **Engage constructively on freedom of association and trade unions:** Since trade unions are unlikely at present to be able to provide information to workers about their labour rights, ICT companies should provide relevant information to employees and other workers, particularly in light of the many new labour laws. Given non-existent or only nascent awareness and understanding of the right to freedom of association and collective bargaining, companies should ensure that their workers are aware of and able to exercise their rights, and engage constructively with trade unions where workers choose to establish them. Moreover, they should ensure that workers who lead or join a union are not discriminated against, dismissed or otherwise impeded in carrying out their trade union functions.
- **Support business partners in respecting labour laws and standards:** Local Myanmar companies will need support in meeting a wider range of contracting requirements around quality, working conditions, health and safety and anti-corruption. Telecoms operators, network equipment providers, tower companies, and the other main contractors should put in place specific contractual requirements together with monitoring, support, training, and relevant incentives and disincentives with business partners supplying goods and services to prompt uptake and respect for relevant international, national and company standards.
- **Pay particular attention to the rights of workers of subcontractors**: Working conditions, including health and safety issues, were raised by workers of sub-contractors met during field assessments. These workers were in lower-skilled, lower paid, manual labour positions, working on a temporary or irregular basis in which working conditions and preventative measures could be haphazard, with unclear access to company-provided health services or facilities.

[469] Ericcson, "Response by Ericsson: Myanmar Foreign Investment Tracking Project", *Business & Human Rights Resource Centre* (last accessed September 2015).
[470] See further: LG Electronics, "Response by LG Electronics: Myanmar Foreign Investment Tracking Project", Business & Human Rights Resource Centre (last accessed September 2015).

- **Exercise vigilance around the continued but declining risk of forced labour:** The ILO is not yet proposing to disband the Forced Labour Complaints Mechanism, indicating an ongoing if decreasing problem.[471] Even though the incidence of forced labour in Myanmar is diminishing, ICT tower construction companies and fibre cable operators in particular should remain vigilant to the potential risks of forced labour. There is still the potential for forced labour by the *tatmadaw* and local authorities in connection with road building and infrastructure construction, although the assessment did not find this is happening in connection with the rollout of the ICT infrastructure.
- **Be alert to and eliminate other forms of labour exploitation:** As a least developed country (LDC) with a high degree of rural poverty; a generally uneducated population; underemployment; corruption and a current lack of worker awareness about their rights and few trade unions, there is a high risk for exploitative working conditions. Many of the jobs for local communities will be in unskilled, daily wage jobs, often controlled via third party labour brokers operating either formally or informally – such as in the construction of the network infrastructure.
- **Be alert to working conditions for migrant and temporary workers:** ICT companies should be aware that while the prevailing pattern has been one of out-migration from Myanmar to other countries in search of work, as the economy develops, that trend may reverse. In any case, internal labour migration is widespread. Migrant workers are often particularly vulnerable to labour exploitation.[472] These circumstances create the possibility of exploitative working conditions and practices that can in some cases fall within the definition of forced labour, where work is undertaken by a person under the threat of a penalty. Workers indicated they are keen for any kind of paid work, so they are often very reluctant to speak out about what can be exploitative working conditions.
- **Carry out due diligence on labour brokers/labour agencies**: ICT companies will need to pay careful attention to the working arrangements and conditions for day labourers or temporary workers engaged through a third party labour agency or broker (who could also be a worker/team leader) to ensure that they are not directly linked to situations of exploitation. The field assessments indicated formal recruitment agencies and labour brokers are not yet commonly visible in network rollout operations. However they are present in other industries (e.g. pipeline construction) where various sub-standard practices have been observed, including not providing basic protections for workers, such as failure to uphold basic working conditions, provide written and understandable contracts, or pay a living wage, and charging workers for PPE provision (see the Oil & Gas Sector-Wide Impact Assessment, Part 4.4) [473]. International labour standards prohibit labour brokers from taking fees from workers for job placements; instead, any placement fees should be paid by the employer. While the Myanmar Government has not ratified the relevant ILO Convention,[474] it is a global standard in this emerging area of human rights risk that serves a relevant guide for company practice. Employers should:

[471] The ILO reports a reduction in occurrences generally throughout the country but notes that "forced labour remains a problem," and that the "number of reported cases of forced labour in the private sector is relatively small … but that this does not necessarily reflect the actual situation as there appears to be a general belief that forced labour is in some way an offence committed only by the Government." ILO, "Update on the operation of the complaint mechanism in Myanmar" GB.319/INS/INF/2 (October 2013).
[472] See the IHRB, *Dhaka Principles for Migration with Dignity*.
[473] MCRB, IHRB, DIHR, "Myanmar Oil & Gas Sector-Wide Impact Assessment" (2014).
[474] ILO, *C181 - Private Employment Agencies Convention* (No. 181) (1997).

- set in place a clear recruitment policy for hiring of staff or use of labour brokers
- ensure that supervisors and managers are aware of the signs of exploitation
- pay the recruitment fees for workers themselves and prohibit accepting payments or other inducements from labour brokers or workers
- monitor the allocation of jobs and use of agencies for signs of suspicious practices
- ensure that all workers, including temporary workers, have access to a grievance mechanism to complain about potential or actual violations of their labour rights

- **Monitor business relationships**: ICT companies should monitor business partners to ensure that they are upholding national labour laws and international labour standards, including through regular surprise field visits. The risks of labour rights violations tend to increase with each tier of the supply chain, where workers are in lower-skilled, lower paid, manual labour positions which are temporary or irregular.

Child Labour

- **Monitor business partners for child labour violations:** While there is a very low likelihood of child labour in direct employment situations within skilled operations of the ICT sector, the prevalence and general acceptance of child labour in Myanmar and the difficulties of validating age means that companies need to be vigilant. Companies should be alert to the possibility of child labour being used in supplying products or services, such as in construction or catering, directly linked to their operations. There are an increasing range of tools available to assist companies in assessing risks to children from their operations.[475] (See also Chapter 4.8 on Groups at Risk).

Discrimination

- **Seek to increase female representation in the workforce:** Dscrimination against women and girls in education and the workplace is widespread in Myanmar.[476] The current rate of female employment in the ICT sector is low, as it is in many other countries. (See also Chapter 4.8 on Groups at Risk).
- **Be alert to ethnic and religious discrimination in the workforce:** Companies need to be aware of the potential for ethnic and religious tensions and discrimination in recruitment and in the workplace. The ethnicity or religion of company managers, particularly in human resources, can have significant consequences.[477] Workers' ethnicity/religion will not be readily apparent, particularly to non-Myanmar managers. However it may not be wise for employers to collect data on the religious and ethnic make-up of their workforce; this may create more tension. Furthermore, many Myanmar people are of mixed heritage or self-identify in various ways. A better approach may be management awareness of the sensitivities, clear company policies on non-discrimination, reinforcement of those messages and modelling an approach to equal opportunities that includes active measures to achieve those outcomes. There are few easy answers on how to address hostility that may spill over into the

[475] UNICEF and the Danish Institute for Human Rights, "Children's Rights in Impact Assessments - A guide for integrating children's rights into impact assessments and taking action for children" (2013).
[476] For example, in Coca Cola's report to the US State Department on its activities in Myanmar, the company highlighted that it found that women were being paid approximately 11% less than male colleagues for the same work.
[477] From IHRB, "From Red Flags to Green Flags: The corporate responsibility to respect human rights in high risk countries" (2011), pg. 73-76.

workplace; specialised expertise and re-emphasising a commitment to non-discrimination are a good place to start.

- **Community composition considerations:** Companies should aware of the ethnic composition of communities where they operate and from where they may recruit workers. Myanmar's ethnic minorities make up an estimated 30 – 40% of the population, and ethnic states occupy some 57% of the total land area along most of the country's international borders.[478] One location may have a mixture of ethnicities. For example there are many different ethnic groups in Shan State besides the Shan, including the Pa-O, Palaung (Ta-ang), and Bamar. Kayin State comprises other groups besides Kayin, including Mon, Pa-O and Bamar. Different ethnicities have different languages and traditions, which need to be taken into account in the workplace. This is especially important given the current rollout phase and expansion into new ethnic minority areas. As of March 2015, nearly 250 towers are planned for construction in Northern Shan State. 300 are planned for Rakhine state, and over 350 in Kachin State.
- **Take the opportunity to increase employment of people living with disabilities:** People living with disabilities are an invisible but substanial group in the Myanmar population and even more invisible in the workforce. As in many other countries, it requires positive steps by employers to recruit and retain disabled workers, and help them to become an integrated part of a workforce not accustomed to disabled co-workers.[479] Where possible, companies may consider incorporating the principles of universal design (defined as the design of products, environments, programs and services to be usable by all people, to the greatest extent possible, without the need for adaptation or specialised design). (See also Chapter 4.8 on Groups at Risk).
- **Be alert to discrimination against lesbian, gay, bisexual and trans-gender (LGBT):** Employers need to be aware of discrimination against LGBT people in the workplace and society more generally, and the fact that same-sex relationships are still criminalised in Myanmar. (See also Chapter 4.8 on Groups at Risk).

Health & Safety

- **Focus on safety in network construction:** There is a clear need for greater attention to basic health and safety throughout network construction activities, particularly tower construction and fibre cable digging. The field research indicated that in numerous operations, there was a failure to meet even the most basic health and safety provisions such as drinking water, and personal protective equipment (PPE). There are clear challenges in transmitting standards to subcontractors' and other business partners. Companies need to use contractual requirements, monitoring and support to build the awareness and skills of local where around HSE management. Myanmar has few labour inspectors and installations often take place in remote areas, where self-regulation by the ICT companies as the only safeguard. Thus it is even more incumbent on the sector to provide safety equipment and take strict safety measures. More robust protection is required in post- and active conflict areas, especially where armed groups may be active near site locations, or where there are risks of land mines around infrastructure.[480]

[478] Transnational Institute/Burma Centrum Netherland "Access Denied: Land Rights and Ethnic Conflict in Burma" (May 2013).
[479] See MCRB and Deaf Resources Centre Guide, "Corporate Social Responsibility and Disability (CSR-D) – A Guide for Companies" (2014). See also, ILO "Disability in the Workplace: Company Practices" (2010).
[480] A concern which was raised during the consultations to the World Bank "Myanmar - Telecommunications Sector Reform Project: environmental and social management framework" (2013), pg 63.

- **Address other sector-specific health and safety risks:** There are a number of sector specific occupational health and safety risks in connection with the installation of communications equipment, such as exposure to electrical fields, electromagnetic fields (EMF) and exposure to laser light during cable connection and inspection activities or working at elevations.[481]
- **Address public concerns about health impacts of mobile phones:** One of the most commonly cited public concerns is over the potential health effects associated with exposure to EMF (such as from mobile phone base stations). To date, there is no empirical data demonstrating adverse health effects from exposure to typical EMF levels from power transmissions lines and equipment[482]. However, the WHO will conduct a formal risk assessment of all studied health outcomes from radiofrequency field exposure by 2016.[483] Exposure to the radiofrequency fields emitted by mobile phones is generally more than a thousand times higher than from base stations, so the greater likelihood of any adverse effect from handsets means that research has almost exclusively been conducted on possible effects of mobile phone exposure.[484] However, two international bodies have developed exposure guidelines for workers (and the general public), based on a detailed assessment of the available scientific evidence, albeit they are now quite dated (2005 and 2009 respectively). [485] There is no data available on whether Myanmar has EMF standards for workers[486] which means that companies should use appropriate international or regional standards for appropriate safeguards for workers.
- **Address other health risks:** The rollout of telecommunications infrastructure across the country requires frequent use of motor transport. Give the poor state of Myanmar's roads and the steadily increasing rate of motor accidents and fatalities,[487] companies should prepare and implement motor vehicle safety programs to protect the safety of their workers and the communities in which they operate.[488] In some countries long-haul truckers have significantly higher rates of sexually transmitted diseases than the host communities. A specific education and training program for transportation contractors may be necessary if there are a lot of trucking services to be used.

---

[481] For a discussion and suggested safeguards, see IFC, "Environmental, Health, and Safety Guidelines – Telecommunications" (2007), section 1.2.
[482] Ibid.
[483] WHO, "Electromagnetic fields and public health: mobile phones" *Fact sheet N°193* (October 2014). The fact sheet lists the "Key Facts" as follows: **"***Mobile phone use is ubiquitous with an estimated 6.9 billion subscriptions globally; The electromagnetic fields produced by mobile phones are classified by the International Agency for Research on Cancer as possibly carcinogenic to humans; Studies are ongoing to more fully assess potential long-term effects of mobile phone use; WHO will conduct a formal risk assessment of all studied health outcomes from radiofrequency fields exposure by 2016."*
[484] WHO "What are the health risks associated with mobile phones and their base stations?**"** (20 September 2013). An earlier WHO 'Backgrounder' on basestations and wireless technology from 2006 noted: "*Recent surveys have indicated that RF exposures from base stations and wireless technologies in publicly accessible areas (including schools and hospitals) are normally thousands of times below international standards*."
[485] Institute of Electrical and Electronics Engineers (IEEE), "Standard for safety levels with respect to human exposure to radio frequency electromagnetic fields, 3 kHz to 300 GHz, IEEE Std C95.1" (2005) and International Commission on Non-Ionizing Radiation Protection (ICNIRP), "Statement on the Guidelines for limiting exposure to time-varying electric, magnetic and electromagetic fields (up to 300 GHz)" (2009).
[486] WHO, Global Health Observatory, Legislation, "EMF Standards" (accessed 28 April 2015).
[487] UNESCAP, "Present State of Road Safety in Myanmar" (2013).
[488] See, IFC "General Enviornmental, Health and Safety Guidelines" (2007), section 3.4.

Expectations of Local Employment

- **Be aware of different perceptions of 'local':** There are high expectations of employment from local communities. According to the *2012 Foreign Investment Law*, all unskilled workers must be Myanmar nationals. While companies may meet 'local hire requirements' by hiring workers from other parts of Myanmar, for local communities 'local' hiring means from the immediate area. This mismatch in terminology and perceptions may create longer-term tensions around projects. Genuinely 'local' workers are likely to be frustrated with the limited numbers and levels of jobs available which will be largely unskilled, low wage and temporary, as they lack relevant skill sets.

D. Relevant International Standards and Guidance on Labour Issues

Relevant International Standards:

- IFC Performance Standard 2 and Guidance Note – Labour and Working Conditions
- IFC General Environmental, Health and Safety Guidelines
- IFC/World Bank Group Environmental, Health, and Safety Guidelines for Telecommunications
- ILO, Declaration on Fundamental Rights and Principles at Work
- UN Guiding Principles on Business and Human Rights

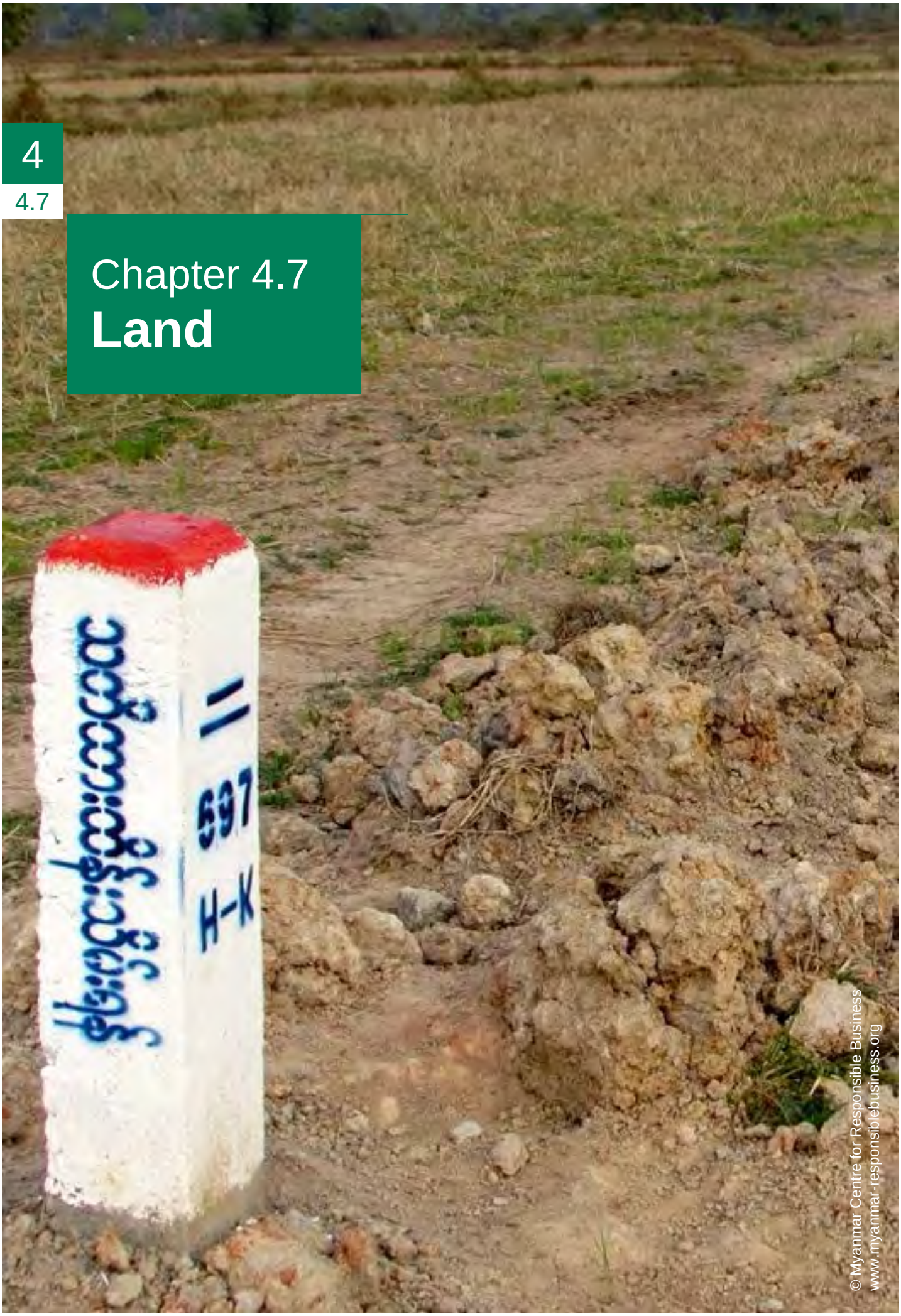
Relevant Guidance:

- IFC:
  - "Good Practice Note: Non-Discrimination and Equal Opportunity"
  - "Good Practice Note: Workers' accommodation: processes and standards"
  - "Measure & Improve Your Labor Standards Performance: Performance Standard 2 Handbook for Labor and Working Conditions"
- IHRB:
  - "Dhaka Principles for Migration with Dignity"
  - "ICT Sector Guide on Implementing the UN Guiding Principles on Business and Human Rights"
- ILO:
  - "Indicators of Forced Labour"
  - "Combating forced labour: a handbook for employers and business"
  - "The Labour Principles of the UN Global Compact – A Guide for Business"
  - ILO pages on Postal and Telecommunications Workers
- Verite, "Help Wanted programme and Fair Hiring Toolkit"

4

4.7

Chapter 4.7
Land



Chapter 4.7
Land

In this Chapter:

A. Context

Land is often the most significant asset of most rural families in Myanmar. An estimated 70% of Myanmar's population lives in rural areas and is engaged in agriculture/aquaculture and related activities.[489] Many farmers use land communally (that is, share the use of land amongst themselves), establishing longstanding land use patterns informally by custom rather than law.[490] These customary land tenure systems are especially prevalent in upland areas inhabited by ethnic minorities. Because much of Myanmar's rural land is not formally registered, land use is characterised by weak or non-existent protection of usage rights and tenure for small-scale farmers, communities, ethnic minorities and other groups at risk of land expropriations.

Since the recent political reform process began in 2011, there has been consistent reporting of protests against 'land grabs'[491] in many parts of the country in the press and by non-Governmental organisations. In addition, large-scale land allocation by the Government has increased significantly in the past decade.[492] While some of these 'land grabs' are new, many of them originate in land expropriations under the previous military Government, a legacy which Myanmar people are now challenging, including through mechanisms provided by the Government. Some land in Myanmar has been returned to farmers and others since the reform process began. However, there are still tens of thousands of rural people who have lost their land due to Government expropriation. Moreover, dozens of farmers and land rights activists have been arrested recently for peacefully protesting against land expropriations by the authorities.[493] There have also been several land disputes in major metropolitan and semi-rural areas. For example in the Thilawa Special Economic Zone near Yangon, dozens of families have had their land

[489] See UNDP, "About Myanmar" and CIA, "World Factbook, Burma, Economy"(last accessed August 2015).
[490] Transnational Institute, "Access Denied" (May 2013), pg 11.
[491] The term 'land grab' in Myanmar is used to cover a wide range of situations, including land disputes and government/military expropriation of land for companies and its own use.
[492]OECD, "OECD Investment Policy Reviews: Myanmar 2014" (March 2014), pg. 324.
[493] See for example Amnesty International "Annual Report 2014/2015, Myanmar country entry" (Feb 2015).

expropriated by the Government and have protested about the deprivation of livelihoods and inadequate conditions in their resettlement area.

In addition to the significant confusion caused by different types of land tenure systems in the country, Myanmar has large displaced communities that retain a claim to their lands, even though they do not currently have possession. Some ethnic minorities in the east of the country have been displaced for decades, leading to very weak tenure over their original land, which they may not have occupied for years, and may now be used by others. More recently, since mid-2011 some 200,000 ethnic minority civilians have been displaced in northern Myanmar as a result of ongoing internal armed conflict, and almost 140,000 have been displaced by inter-communal violence in Rakhine State since June 2012. These newly displaced populations may not be allowed to occupy and use their land when they attempt to return to it.

As a result, ascertaining the provenance of land ownership in Myanmar is not straightforward: existing land records may not reflect true ownership; many people do not have sufficient documentation of their land rights; and many have claims to land through customary land tenure systems which are not officially recognised by the Government.[494]

Land Use for the Telecommunications Sector

ICT companies will usually lease (or for some local companies potentially purchase) land for their operations, whether it is for offices, ICT parks or infrastructure development. Compared to some of the sectors increasing their operations in Myanmar such as agriculture and mining, the ICT sector has a smaller and far more dispersed land footprint. The infrastructure is characterised by small tower sites (although nearly 8,000 towers are planned for 2015) as well as over 5,000 kilometres of narrow trenches for laying cable and fibre. The remainder of the footprint is essentially office space for day-to-day operations across the sector, some of which has been grouped together into 'ICT Parks'. There is negligible manufacturing in the sector so this part of the value chain currently has no footprint to speak of but could increase. For the most part, the 'over the top' services sector does not have a physical presence in the country. SIM cards and equipment are distributed through a myriad of small shops, often selling a wide range of goods.

Tower construction companies acquire land for towers by leasing the land from the owners for a long-term period of typically 15 years.[495] A mobile operator publicly commented that the Government had set a fixed price for leasing land held by ministries or administrative bodies (such as Yangon City Development Corporation in Yangon) if leased for tower construction.[496] The specific price is not public.

As detailed below, companies ask permission from the owners and their immediate neighbours to rent the site and then construct and operate the towers. Some of the land being used for towers is paddy land,[497] which is protected for food security reasons and cannot easily be converted to other uses. Moreover, permission for conversion of paddy land on which rice is being grown needs to be granted by the national level authorities

[494] For a more detailed discussion of land issues, see: Myanmar Centre for Responsible Business, "Briefing Paper on Land Issues in Myanmar" (March 2015).
[495] Myanmar Times "Ooredoo builds 100 towers as launch looms closer, (26 May 2015).
[496] Telenor, "Myanmar Sustainability Briefing" (12 May 2015).
[497] *Myanmar Farmland Management Rules*

before it can be reclassified for other uses. This slows the process considerably, and increases the opportunity for officials to ask for bribes as the requests move through various levels of bureaucracy. Tower companies have been helping landowners to get the land reclassified from paddy land to grant land[498] so that it can then be leased out.

Some of the land used for towers is farmland (other than paddy land) which also requires a conversion process to change the designation, but this can be done at the state level. Even in urban areas, the lack of proper land documentation is causing delays. Companies and authorities are also confused about what documents are needed to change land registration status and to register long term leases, resulting in delays. .

The companies laying fibre/cable are digging trenches, laying fibre/cable, then covering the trenches. As such, they are not entering into lease arrangements but instead may be making a one-time payment for the disturbance of the land, usually without further formal arrangements.

Several tower companies have joined together to highlight identified bottlenecks in the current processes to use of farmland for the placement of towers, the registration of leases and the use of Government land, and have proposed several solutions to the authorities to expedite the process.

World Bank Guidance for Land Use by the Telecommunications Sector

The World Bank is currently financing and implementing a $31.5 million telecommunications sector reform project in Myanmar that includes a programme to extend coverage in selected remote pilot locations that are commercially non-viable for operators to service without a one-time subsidy and are not part of the networks being rolled out by the licensed operators.[499] It has a set of environmental and social safeguard policies [500] that apply to most World Bank projects and that are applicable to this telecommunications sector reform project. As part of the environmental and social management framework (ESMF)[501] for the project, the World Bank developed a set of land lease guidelines for the roll out of pilot telecommunications infrastructure in rural areas[502]. All sites where telecommunication masts/ towers will be installed to extend connectivity will be selected and managed in line with the ESMF.

As the ESMF notes *"[r]ecognising that land markets are poorly developed and there are few or no experiences with land leasing arrangements for telecommunications towers and masts in Myanmar, principles for such arrangements have been developed under this ESMF*" because "*tenure rights are rapidly evolving in rural Myanmar*". The Guidance notes that because land tenure is not fully established in rural Myanmar and rural

[498] Grant land is "Owned and allocated by the state, grant land is common in cities and towns, but rare in village areas. The state may lease grant land out for extendable periods of ten, thirty, or ninety years. Grant land is transferable, is subject to land tax and may be reacquired by the state during a lease period in accordance with laws governing compulsory acquisition." USAID, "Property Rights and Resource Governance: Burma" (date unknown) pg. 10-11.
[499] World Bank, Telecommunications Sector Reform Project (last accessed August 2015).
[500] World Bank, "Consultations on the Second Draft of Environmental and Social Framework" (1 July 2015).
[501] Myanmar - Telecommunications Sector Reform Project: environmental and social management framework (2013). The Environmental and Social Management Framework describes the baseline project environmental conditions and impact, provides guidance for environmental and social assessment processes.
[502] World Bank, "Myanmar - Telecommunications Sector Reform Project: environmental and social management framework (Vol. 2): Land lease guidelines" (English) (2013).

populations may have informal claims to the land, care should be exercised to clarify if indigenous claims to lands identified for housing infrastructure exist – and whether any individuals use the land to gain a livelihood – before a decision is made to determine where infrastructure should be built. The series of steps set out are intended to mitigate impacts on rural communities.

When building their infrastructure in accordance with the ESMF, the rural telecommunications service providers are expected to make a long-term lease contract on a commercial basis with willing land owners/occupants. The procedures require verification of all land leases being carried out with appropriate arrangements and on a commercial basis, without coercion or under duress, and with no legacy issues in any land transactions. If land markets are underdeveloped in the pilot area, as will be the case for most pilot sites, the lease fees should be set at a price that will be broadly sufficient to cover the long-term livelihood loss as a result of the leasing.[503] The project will not ask the Government to acquire land by exercising its power of eminent domain, nor will the Government be asked to move people involuntarily. The rural telecommunications service providers will be expected to put in place feedback mechanisms to handle grievances and compliance will be monitored by the World Bank task team.

Land Policy Framework

Reform of land policy and law in Myanmar remains incomplete. The current land regime is characterised by a patchwork of new and old laws that often leads to overlap, contradiction and confusion for current and prospective owners and users. Moreover, the land registration system is considered inefficient and insufficient, with complex requirements and lack of benefits for registering land.[504] The cadastral (land mapping) system is outdated, which further exacerbates land disputes, as land classifications and mapping used by different Government ministries may overlap nor reflect current land use patterns.

Land in Myanmar is classified into several different categories, including Freehold Land, Grant Land, Reserved Forest Land, Farmland, Grazing Land, Religious Land, among others. This means for example that a plot of land may be classified on maps as Reserved Forest land, when in fact the land may now be used as farmland, without a change in the classification.[505] As a result, land tenure rights – the right to use, control, or transfer land[506] – are often insecure, posing a major problem.

The new land laws[507] do not sufficiently recognise customary land rights or the rights of informal land occupiers or users who lack formal documentation of their 'usufruct' rights (i.e. individual rights to use and enjoy the property of another).[508] Experts have recommended that the Government formally recognise customary law for land use rights and provide mechanisms for communal ownership of land to ensure *inter alia* ethnic

[503] Ibid.
[504] OECD, "OECD Investment Policy Reviews: Myanmar 2014" (March 2014), pg 108.
[505] Food Security Working Group's Land Core Group, "Legal Review of Recently Enacted Farmland Law and Vacant, Fallow and Virgin Lands Management Law", (Nov. 2012), pg. 7-10.
[506] FAO "What is land tenure" (last accessed September 2015).
[507] *Myanmar Vacant, Fallow and Virgin Lands Management Law* (2012) and *Farmland Law* (2012). See for further description, Land Core Group, "Legal Review of Recently Enacted Farmland Law and Vacant, Fallow and Virgin Lands Management Law" (Nov. 2012).
[508] "*…the written and unwritten rules which have developed from the customs and traditions of communities…*" Ibid. pg. 15-16.

minority rights are protected.[509] In addition, the Government may be declaring land vacant that in reality is not. This has resulted in large numbers of landless who would not appear in any Government records but who may nonetheless be affected by displacement. They should be compensated for at least economic displacement if they have lost their livelihoods. Further livelihoods support could be addressed through social investment programmes.

It is expected that demands for land will inevitably increase with further economic development and investment. There is a recognised need in Myanmar for a written National Land Use Policy and comprehensive umbrella national land law. To that end, a working group of a Government committee which included civil society representation and external experts formulated a draft Land Use Policy. The 6th Draft of the Policy was published in May 2015 for further consultations among a wide group of stakeholders.[510] The draft National Land Use Policy is expected to be sent to the President after further meetings took place at the end of June 2015.[511] The Policy will reportedly guide the drafting of an umbrella Land Law, also expected to be discussed during public consultations. However, a new "*Land Law"* will not be passed by the current Parliament in 2015. While the development of such an overarching policy document is a needed and welcome step, civil society in Myanmar fear that poor farmers' land rights will not be adequately protected under the new Land Use Policy.[512]

Legal Framework for the Acquisition or Lease of Land[513]

Acquisition by/with the Myanmar Government

The 2008 Constitution provides that the State is the ultimate owner of all land in Myanmar, but also provides for ownership and protection of private land property rights.[514] The Government can carry out compulsory acquisitions in the state or public interest (see below). A private investor may acquire land or land use rights from either the Government or from a private land owner. A foreign investor can lease land.

With respect to lands not covered by other, more specific land laws (either the 2012 *Vacant, Fallow and Virgin (VFV) Land Management Law* or the 2012 *Farmland Law* – see below), land acquisition is governed by a 120 year old law, a holdover from the former British colonial period. The 1894 *Land Acquisition Act* provides that the Government can carry out land acquisitions for a company when the acquisition is "*likely to prove useful to the public*" (Article 40(1)(b)). The Government has responsibility for carrying out the acquisition and distributing compensation but the funds for compensation are to be provided by the company acquiring the land. Land in kind can be provided in place of monetary compensation. The law sets out basic procedures governing the acquisition of the land, including undertaking preliminary investigations on the land, and a procedure for notification of, and objections to be raised by, persons interested in the land.

[509] Ibid, pg. 23-24.
[510] 6th Draft of the National Land Use Policy, English version, May 2015, on file with IHRB/MCRB.
[511] Myanmar Times "Delayed land-use forum scheduled for June" (29 April 2015).
[512] Irrawaddy "NGOs, Farmers Concerned After Reviewing Draft Land Use Policy" (1 November 2014).
[513] For a more detailed discussion of the legal framework for acquiring land, see Myanmar Centre for Responsible Business, "Land Briefing" (March 2015).
[514] *Myanmar Constitution* (2008), Articles 35, 37, 356 and 372.

VFV Lands Management Law and the Farmland Law

The 2012 *Vacant Fallow and Virgin (VFV) Lands Management Law* and *VFV Rules* are clearly aimed at providing a legal framework for implementing Government land policies to maximise the use of land as a resource for generating agricultural income and tax revenues. Tenure security is deliberately circumscribed to allow the Government the flexibility to do what they believe is needed for development. Civil society groups and farmers organisations have pointed out that land regarded as VFV may in fact be occupied by people or subject to shifting cultivation according to traditional farming practices, but which the Government classifies as "*vacant*" under the VFV. The complicated registration procedures under the 2012 *Vacant Fallow and Virgin (VFV) Lands Management Law* and the 2012 *Farmland Law* mean that smallholder farmers, a large percentage of Myanmar's population, will struggle to register their land tenure claims and are at risk of having their land registered by more powerful interests. By not recognising informal land rights, and formalising land rights through titling despite pre-existing informal claims, the new laws may reinforce existing inequality and/or create new injustices. This has potential to create or exacerbate tensions and disputes.[515]

With respect to farmland, the 2012 *Farmland Law* makes clear that applicants who are individuals must be citizens (Articles 6(a)(v), 7(a), (iv)). Under the 2012 *Foreign Investment Law* (FIL), there are restrictions on foreign investment in agriculture under Article 4(h), but Article 5 provides for the Myanmar Investment Commission, with approval from the Government, to allow investment.[516] The 2012 *Farmland Law* also allows for the repossession of farmland "*in the interests of the state or the public*"[517] provided that "*suitable compensation and indemnity is to be paid and the farmland rights holder must be compensated "without any loss*" (Article 26). As with the *VFV Law*, the *Farmland Law* and *Rules* do not provide for procedures for objections to be made to the acquisition or compensation awarded, or for judicial review.

Non-Citizens' Use of Land

Private investors may acquire land rights from private persons through ordinary contractual agreement, subject to the following legal restrictions. First, land ordinarily cannot be sold or transferred to a foreigner through private transaction.[518] The Government may however allow exemptions from these restrictions and *Union Government Notification No. 39* of 2011[519] sets out the circumstances in which a foreign investor may lease land. Second, private investors cannot acquire VFV land rights or farmland through private transactions without the permission of the Government (Article 16(c) *VFV Law*) (Article 14 *Farmland Law*). Under the 2012 *Foreign Investment Law*, foreign investors can obtain leases for an even longer period, 50 years, extendable for 10 years twice, depending on the type of business, industry and amount of investment. Leases can be even longer for land in "*the least developed and less accessible regions*".[520]

---

[515] Transnational Institute, "Access Denied: Land Rights and Ethnic Conflict in Burma", (May 2013)
[516] *Myanmar Foreign Investment Law 2012*.
[517] The distinction drawn between interests of the state and interests of the public is troubling, but it may be premature to draw conclusions without knowing the nuances of the provision in Burmese.
[518] The 1987 Transfer of Immoveable Property Restriction Act prohibits the sale or transfer of immoveable property, and the lease of such immoveable property for more than one year, to a foreigner or foreigner-owned company (Articles 3-5).
[519] Notification 39/2011 on the Right to Use of Land relating to the *Myanmar Foreign Investment Law*.
[520] Ministry of Planning and Economic Development, "Notification 11/2013, Foreign Investment Rules", (31 Jan 2013).

It should be noted that the 2012 *Foreign Investment Law* and the 2013 *Citizens Investment Law* are currently being redrafted to create a single law for all investors and these provisions could change.[521]

Resettlement

Myanmar has only limited standards governing the resettlement process for land confiscated from people for projects. As discussed above, the *1894 Land Acquisition Act* does provide for compensation for land the Government has acquired in the public interest, but with only limited safeguards and no provisions concerning resettlement. In addition, the current *Foreign Investment Rules* appear to provide some general prohibitions on involuntary resettlement.

B. Field Research Findings

The field research focused on parts of the ICT value chain where land acquisition processes were most significant (for infrastructure roll out)[522] and where land owners or users were most at risk (i.e. rural communities). It did not consider land acquisition for office use in cities where land registration and markets are more developed. The findings are based on the roll-out experience of private sector telecoms operators. While the field research team discussed land acquisition with state-owned enterprise MPT, the team did not have the opportunity to discuss land acquisition with military-owned enterprise MECtel. MECtel usually locates infrastructure inside military compounds or on land held by the military.

Consultation Prior to Land Acquisition

Human Rights Implicated: Right to take part in the conduct of public affairs; Right to information

Field Assessment Findings

- There were numerous cases where individuals and communities claimed there was **no informed consultation and participation** about land acquisitions or tower or fibre projects using land in immediate proximity to their homes.
- In cases where there was consultation and participation, it was predominantly **only with the land owner/user and the (two to four) immediate neighbours,** who, under the land acquisition process, were needed to sign consent forms. In many of those cases, **those asked to sign agreements were unclear of their purpose or content.**
- There were **very few cases** found where any ICT company or Myanmar Government had done **wider community consultation regarding the network rollout,** land needs and plans, and the ways in which the rollout would affect their lives and livelihoods, positively or negatively.
- In many cases, community members:

[521] Myanmar Centre for Responsible Business "Comments on the latest draft of the Myanmar Investment Law" (27 March 2015).

[522] For example, TowerXchange reports in October 2014 that "*based on the volume of orders they are seeing, the tower installation firms have spoken to are more bullish than the GSMA's forecast of 17,300 towers by 2017, with many feeling that the tower count in Myanmar by 2017 will be 25,000*". TowerXchange "The Myanmar tower rollout: FAQs" (updated June 2015).

- received **no prior information about the intention to acquire their land or land near their homes**, only understanding the reason was to build a tower or lay the cable line once it became apparent during construction or digging
- were **not consulted** or given an opportunity to become informed about the **broader project of building the network**. Instead, information was given only with respect to the land registration process (see Due Process below) and compensation
- were given **no choices** or opportunity to negotiate about the plot of land or restrictions on land use
- often **did not know for which telecom operator** the tower construction company was building, or the cable line was being dug
- were **not given any information to make contact or complain** either with the cable laying company, tower construction company or telecom operator
- It was a regular occurrence for communities to **host tower construction managers and/or groups of workers, in their homes** during the build period, without compensation for the accommodation, water or laundry use. While this was by agreement, it often lasted for a period longer than originally agreed and some cases involved more workers than agreed and/or also their spouses and children (and sometimes pets)

- **Commonly raised community concerns included:**
  - **not knowing which company was involved** in the construction (whether fibre cable or tower)
  - **not having a company contact** in cases of problems or emergencies
  - **not being provided with basic information on the safety of the tower** including:
    - whether the tower could withstand earthquakes or severe weather
    - whether they would be subjected to unsafe levels of radiation from the tower
    - whether they would be electrocuted by the tower during rain showers
  - **noise from generators powering the towers** causing a disturbance, headaches, and small cracks in walls/floors
  - **tower sites being fenced in but not locked**, compelling villagers to "*guard*" the site to ensure children or others do not wander in
- Community members expressed a desire for **strong mobile phone reception** (which comes with good tower coverage) but **did not want towers built nearby their villages** – which reflects the common NIMBY ('not in my backyard') phenomenon.
  - There was also the perceived dilemma of the benefits of regular income from lease payments versus concerns about health risks from living near a mobile phone tower.

Due Process in Acquisition

Human Rights Implicated: Right to not be arbitrarily deprived of property; Right to an adequate standard of living; Right to freedom of expression

Field Assessment Findings

- The field assessment findings **affirmed the complexity and opacity of the land acquisition process and regulatory framework** outlined in the National Context section above for the tower companies and land owners.
- Some called for a **model lease contract template, approved by the authorities**

and **available in local languages**.

- Reports were received of **construction taking place on paddy land or farmland**, **without the necessary documentation, including land conversion approval**. Private companies noted that receiving the land conversion approval for farm or paddy land was "*impossible*" due to administrative delays, bribery, and in some cases farmers lacking requisite documentation needed to apply for the conversion. However a regional-level minister expressed awareness of the complexity of the approval process, and suggested that regional-level Government is working to ease the process for both landowners and companies engaged in the roll-out.
- **For tower construction**, interviews indicated a **relatively consistent process was followed by most companies that resulted in a signed lease for land owners**:
  - A 'site hunter' comes to the home/farm to investigate the land and suitability for a tower site.
  - If suitable, they discuss with the village leader/administrator their intention to build on the land, how much land they will need (usually about 50 square metres) and where, how long construction will take (usually a 28 day target), and their rental and compensation rates.
  - The village leader/administrator and site hunter(s) discuss with the land owner their intention to build the tower:
  - The company usually facilitated the process of getting the land registered as "*grant land*" under the required Form 105. (If paddy land, this was first applied for at regional level, then approved at national level before it could be issued). This generally took 1-2 months
  - The landowner must get the signed consent of (usually 2-4) immediate neighbours confirming they do not object to the construction
  - A contract (usually a land lease) is signed between the landowner and company.
- **Fees and costs for registering as grant land** were generally incorporated into the lease agreement (not putting land owners out of pocket), but the **fees and costs cited varied greatly** from 500 MMK ($0.46) up to 40 MML ($3,709), by location.
- It was often the tower site hunter's or village leader/administrator's job to **verify who was the true land owner**:
  - Citizenship Scrutiny cards, Household Lists, and land titles were cited as among key initial documents sought. However, there are still high risks of misidentifying 'true' land ownership in Myanmar even using such evidence, given wide-spread practice of customary ownership and the fact that Myanmar only recently completed its first census in 30 years, which is still widely regarded as problematic because *inter alia* people in some areas of armed conflict and inter-communal violence were not counted.
  - Depending on the circumstances, companies may bring in local lawyers to meet the land owner and assist them in applying for the needed documents.
  - Researchers heard general estimates that around 10% of prospective sites fail because documents cannot be obtained.
  - Researchers heard of some cases in which Myanmar officials obliquely requested bribes in order to return the proper documentation.
- Though contracts were commonly signed with landowners confirming the lease arrangements, a **copy of the contract was often not provided to the land owner** and researchers were regularly told by **land owners that they did not fully understand the content of what they were signing**.
  - Most contracts appeared to include **automatic renewal clauses**, meaning unless the landowner gives notice of their wish to cancel or renegotiate the agreement prior to the completion of the agreed term they will automatically be

tied into a renewed term.

- As companies involved in **laying fiber** were not using land for an extended period of time, they did not use more formalised processes or documents to negotiate access. **One time compensation for disturbance of land was sometimes paid.**

Compensation for Land Acquisition and Use

Human Rights Implicated: Right to not be arbitrarily deprived of property; Right to an adequate standard of living; Right to an effective remedy

Field Assessment Findings

- **Compensation rates for rental of tower sites varied greatly** (including both rooftop and ground towers), **from 2 MML monthly ($185) up to 72 MML ($6,676) monthly,** depending on the location and the land tax to be paid**.**
- **Most landowners were agreeing to lease periods of 10-15 years** for positioning towers on their land, though periods of 5 and 25 years were also reported. As above, contracts often included **automatic renewal clauses.**
- **Lease payments were usually paid annually**, though some companies paid owners every quarter, some every 6 months and others every 2 years.
  - **Some landowners expressed a preference for larger (e.g. 3 year) up-front payments** in order to have sufficient capital to start a business or new venture.
  - As above, **application fees for registering the land** in order to host the **tower were usually incorporated into the payment for the lease.**
  - Some companies paid additional **monthly security fees to the land owner to look after the tower site.**
- **Most lease agreements included percentage increases**, often 3-5%, every 3-5 years.
- **For fibre construction on religious land** it was found that leases and lease payments were not formalised and no official approval had been required. Instead, companies **simply made donations**.
- **For tower construction on religious land** the formal authorisation required at the township level was obtained. Neighbour consent was also obtained. Stakeholders did report difficulty receiving satisfactory information from company representatives regarding the lease, acquisition, and construction process.
- Most companies seemed to operate according to standard compensation ranges. Some **provided site hunters with financial incentives to ensure lease agreements within the specified ranges**, e.g. allowing them to keep the amount left over between the agreed fee and top of the specified range, or receive a commission for staying within the range.
- A few cases were reported of **lack of compensation for trees/crops cut down** to make room for towers or loss of income from their yields.

Access to Remedy for Land Grievances

Human Rights Implicated: Right to an effective remedy; Right to take part in the conduct of public affairs; Right to information

Field Assessment Findings

- As mentioned above, there were **regular reports of communities and land owners not knowing which company was responsible** for fibre cable digging or tower construction, including whom to contact in cases of emergency or grievance.
- **Cases of noise disturbance from generators powering towers were generally**

resolved, in some cases by the village administrator.

- **Some communities complained of damage by the company of roads, as well as of company-provided road repairs that failed to restore the quality** of the road prior to the company's use**.**

Conflict Areas

Human Rights Implicated: Right to life, liberty and security of the person; Right to take part in the conduct of public affairs; Right to information

Field Assessment Findings

- There were some cases in which companies attempted to negotiate access to areas to lay fibre cables with non-state armed groups (NSAGs). **In some cases a fee was paid for this access.**
- Researchers received reports of cases of operational delays, where local groups, including armed groups, **blocked access to sites, due to lack of consultation at the site level.** While some consultation with local leaders may have been undertaken, this may not have been communicated to or accepted by all stakeholders.
- Researchers observed **fire-arms being carried by NSAGs** present during roll-out in ceasefire areas. While researchers neither observed not heard reports of shots being fired, the presence of fire-arms is a risk for both the civilian population and the company itself.
- Researchers also received reports from workers that they were aware that in the past landmines **may have been sown around infrastructure in conflict areas**. This led workers to avoid walking through certain areas. The measures companies took to protect their workers in such circumstances were unclear.

Myanmar Good Practice Examples:

- **Written lease agreements were regularly signed with landowners for towers** (though, as above, copies were often not provided to land owners or they claimed they did not understand the content fully).
- **Most lease agreements included percentage increases**, often 3-5%, every 3-5 years.
- **Companies often facilitated the registration application process, reducing or removing the burden on landowners**.
- Given the lack of a uniform and accessible land registry, regular reports were received of companies accepting alternative forms of documentation. This can offer a significant protection but can also be a significant risk if this is used to bypass customary owners. As a result, **some companies also seemed to be undertaking more detailed due diligence to identify the 'true' landowners**, including direct discussions with villagers and local authorities.
- One company has reported it leases some 1,000 land parcels for its towers with full written approvals and documentation from landowners.[523]

[523] See further: Apollo Towers Myanmar, "Response by Apollo Towers: Myanmar Foreign Investment Tracking Project", Business & Human Rights Resource Centre (last accessed September 2015).

C. Land Recommendations for ICT Companies

4
4.7

Considerations for Land Acquisition / Use

- **See Chapter 4.9 on Stakeholder Engagement and Access to Remedy** for further recommendations on stakeholder engagement and land acquisition processes.
- **Be sensitive to concerns about 'land grabbing':** There has been extensive reporting in recent years of outright 'land grabs' with little pretence of following the law, and of villagers being deprived altogether of compensation, with or without official expropriation, receiving reduced payment for land, or being denied any recognition of ownership [524] by Government authorities, the military and business. There may therefore be legitimate concern about land grabs in connection with existing and planned ICT projects. Even though the vast majority of land transactions for ICT infrastructure is through long-term leases between willing lessee/lessor, this issue could be a source of tension with local communities and subject of advocacy by civil society groups. Operators and tower companies should expect close public scrutiny of their approach to land issues.
- **Ensure effective, transparent and equitable procedures:** The rollout of the ICT infrastructure has an extensive footprint throughout the country, even if the footprint of each individual transaction is not large. When added together, the network rollout will entail thousands of transactions with thousands of landowners. Companies should adopt consistent and effective procedures for consultation and compensation to make sure that this wide range of people impacted by operations are dealt with equitably and transparently across these many transactions.
- **Provide an easy-to-understand guide to the rollout process**: This should identify step-by-step each part of the construction and rollout process that is understandable by villagers, in their local language.
- **Provide an easy-to-understand guide to the contracting process**: This should include a step-by-step process with checklists that identifies steps, documentation and permitting required that is shared with landowners and local authorities to promote greater transparency. It should provide an easy to understand explanation of the contents of the lease contract. This and any contracting documentation should be provided in local languages and in form that local landowners can readily understand.
- **Recognise customary land titles:** Given the lack of a uniform and accessible land registry establishing land ownership; the lack of recognition of customary ownership; and the significance of land-based livelihoods and attachment to ancestral lands, any approach to land use should recognise those customary rights and deal with customary owners on the same basis as more formal land owners. This requires detailed due diligence to understand who the customary owners are, often with direct consultation with communities and local authorities.
- **Provide or pay for legal assistance for landowners**: Some stakeholders highlighted good practice of providing landowners with legal assistance where there were more

[524] The Land Core Group, a grouping of Myanmar and international NGOs working on land issues, has documented 13 cases of land confiscations in central Myanmar in September 2012 (Land Core Group, "13 Case Studies of Land Confiscations in Three Townships of Central Myanmar" Sep. 2012, on file with IHRB.). Over the last several years the Transnational Institute has focused on land rights problems in Myanmar's borderlands where ethnic minorities live. See for example TNI, "Financing Dispossession, China's Opium Substitution Programme in Northern Burma" (Feb. 2012); TNI, "Developing Disparity: Regional Investment in Burma's Borderlands" (Feb. 2013), and TNI, "Access Denied: Land Rights and Ethnic Conflict in Burma", (May 2013). Myanmar civil society, including those which are ethnic minority-based, have also reported on land grabs without compensation or recognition of customary ownership. The Karen Human Rights Group has documented land disputes and land grabs in Karen areas over a number of years. See KHRG, "Losing Ground: Land conflicts and collective action in eastern Myanmar" (Mar. 2013). The Human Rights Foundation of Monland has also reported on such abuses, particularly at the hands of the military, in ethnic Mon areas. See for example Human Rights Foundation of Monland, "Disputed Territory: Mon farmers' fight against unjust land acquisition and barriers to their progress", (Oct. 2013).

complicated legal issues to address in the land registration or leasing process. It should be made clear in those circumstances whose interests are represented if there are choices or a conflict of interest between the tower company's interest and the landowner's interests. If the legal representative cannot take a neutral position, independent legal assistance should be provided to landowners so that they can make informed choices about disposition of their land and the implications of signing longer-term leases.

- **Ensure farmers are not disadvantaged by lack of paperwork**: Paddy land or other farmland is preferred for tower construction because it is flat and easy to reach. Under the current land classification, it is not allowed to be used for anything other than cultivation without Government approval, which is not always immediately forthcoming. Where towers have been constructed without or before approval, subsequent strict enforcement of land laws could potentially result in farmers being penalised for renting to tower companies, and create a risk to their livelihoods. If farmers are penalised, companies should be ready to put in place remedial compensation to ensure that there is no impact on their livelihoods.
- **Be alert to speculation:** Companies should also be aware that there have reportedly been cases in other sectors involved in land acquisition of speculators moving in to acquire land in areas where it is thought that investment projects may be implemented. These speculators seek to acquire land cheaply from original land users who are unaware of the development, hoping to profit from compensation payments. This can create tensions with the original users, who may feel cheated when land use compensation is subsequently paid

Land in Areas Affected by Armed Conflict & Communal Tension

- See Chapter 4.10 on Conflict and Security.

D. Relevant International Standards and Guidance on Land Issues

Relevant International Standards:

- ILO Convention 169, Indigenous and Tribal Peoples Convention (1989), Part II – Land
- FAO Voluntary Guidelines on the Responsible Governance of Tenure of Land, Fisheries and Forests in the Context of National Food Security (2012)
- The World Bank Myanmar Telecommunications Environmental and Social Management Framework (ESMF) Land lease guidelines (English)
- IFC Performance Standard 5 and Guidance Note – Land Acquisition and Involuntary Resettlement
- The IFC/World Bank Group Environmental, Health, and Safety Guidelines for Telecommunications also provide relevant guidance on siting infrastructure and other aspects of community safety.

Chapter 4.8
Groups At Risk

Chapter 4.8

Groups at Risk

In this Chapter:

A. Context

Myanmar is one of the most culturally diverse countries in Southeast Asia, making for a complex interplay of ethnic identities. Many ethnic minority leaders believe that the Burman (Bamar)-dominated central Government instituted a policy of 'Burmanisation' to suppress ethnic minority cultures, languages and religions, and treat ethnic minorities as 'second-class citizens'.[525] There are also several other groups that are at risk of marginalisation. These groups are particularly vulnerable to the impacts of increasing change in the country, due to poverty; lack of stature to make their voices heard in the process of shaping those changes; and an inability to resist more powerful forces. They risk being left behind in Myanmar's rush to transform itself.

Human Rights Defenders

According to the United Nations, a 'human rights defender' is a term used to describe people who, individually or with others, act to promote or protect human rights. Human rights defenders are identified primarily by what they do. It is through a description of their actions and of some of the contexts in which they work that the term can best be explained.[526] As in most countries, there are many human rights defenders in Myanmar, including people working in civil society organisations (CSOs) and ethnic minority community-based organisations (CBOs), trade union, student and religious leaders, journalists, and Myanmar people working in INGOs and UN agencies.

A vibrant and resourceful network of CSOs and CBOs is active at both the national and local levels in Myanmar, including many ethnic minority-based groups. In the aftermath of

[525] For a further explanation and discussion of these issues, please see Transnational Institute/Burma Centrum Netherlands reports from 2011 to 2013.

[526] See further: Office of the UN High Commissioner for Human Rights.

Cyclone Nargis in May 2008, Myanmar CSOs greatly expanded and organised as they worked to help survivors. They remain a significant positive force in the country and have been able to engage with the Government to some extent. Since 2011 Myanmar civil society groups have been granted a greater degree of latitude by the Government and have taken that opportunity to increase their activities to help people claim their rights.

While many developments since the 2011 reform process have increased the space for human rights defenders to operate, there have been some disturbing recent developments, such as the arrests and imprisonment of several local journalists (see Chapter 4.1 on Freedom of Expression); the continuing arrests of peaceful demonstrators under the 2011 *Peaceful Assembly Law*, many of them protesting against land grabs[527]; and unchecked inter-communal violence. The run-up to the General Elections scheduled to take place in November 2015; the uncertain constitutional amendment process; and the ongoing peace talks with armed ethnic minority groups are all factors which have led and may lead to greater tensions between civil society, including journalists, and the Government, and within civil society itself.[528] Moreover, people staging peaceful public protests in the context of the upcoming elections may be at risk of arrest and imprisonment by the authorities.

Religious Communities

Buddhist and Muslim

After the controversies around how ethnic minorities could identify themselves in the March-April 2014 census, the Government decided not to publish ethnicity and religion data.[529] Analysis of census information reveals that an estimated total of 1,206,353 people were not enumerated in parts of Rakhine State, Kachin State and Kayin State. This represents 2.34 percent of the population. However the number was counted in the overall Myanmar population total figure of 51,486,253.[530]

The percentage of Muslims in the population is also an extremely sensitive issue in the light of recent violence and Buddhist fears of an increasing Muslim population.[531] Muslims, who live in many parts of Myanmar, are a minority of the population. Anti-Muslim sentiment and discrimination are widespread in Myanmar, not only against the Rohingya,[532] a Muslim group living in Rakhine State, but also against other Muslims in different parts of the country. Inter-communal violence between Buddhists and Muslims broke out in Rakhine State during June 2012 but has also affected other areas of the country. Moreover, there has been Buddhist violence against Muslims since June 2012 not only in Rakhine State, but also in Meiktila, and to a much lesser degree in Mandalay and other parts of the country.[533]

---

[527] Burma Partnership and the Assistance Association for Political Prisoners in Burma, "How to Defend the Defenders?" (July 2015).
[528] Myanmar Centre for Responsible Business "Civil Society Organisations and the Extractives Industries in Myanmar – a Brief Overview" (October 2014).
[529] Republic of the Union of Myanmar, "2014 Myanmar Population and Housing Census, Census Report Volume 2-A" (May 2015).
[530] Ibid.
[531] For a discussion of Muslim population figures in the context of the March-April 2014 census, see International Conflict Group, "Myanmar Conflict Alert: A Risky Census", (Feb. 2014).
[532] The Myanmar Government does not accept the term 'Rohingya' and refers to the population as 'Bengali'.
[533] In Meiktila in the centre of the country, over 40 people were killed in March 2013. In July 2014 further inter-communal violence broke out in Mandalay, Myanmar's second largest city, resulting in two deaths and dozens arrested and wounded DVB, "Mandalay riots reveal splintered community, complex agendas" (8 July 2014).

In the wake of the 2012 violence, almost 140,000 people in Rakhine State remain displaced,[534] many of them in camps in extremely poor conditions, most of them Muslim. Muslims living in camps in Rakhine State are not able to travel in order to access employment or health care. Muslims who live in north-western Rakhine State also face longstanding restrictions on movement and cannot leave their townships without official permission, greatly impacting their livelihoods.[535] On 11 February 2015 the President revoked all temporary identity cards, known as White Cards, leaving many Muslims, including Rohingyas, but also some ethnic minorities, without a valid form of identity card, impacting on their ability to travel, obtain employment and vote.[536] In June former White Card holders did not appear on the voter lists and were thus disenfranchised and will be unable to participate in the November 2015 elections.[537]

Some members of the Buddhist Sangha (clergy) in Myanmar lead the '969' movement, which claims, amongst other things, that Muslims are trying to take over the country. The '969' movement encourages Buddhists to boycott Muslim businesses, and has some popular support.[538] Of the two international telecoms companies granted licenses in Myanmar, Ooredoo is based in Qatar, a Muslim-majority country. After the awards were granted, some radical nationalist Buddhist monks called for a boycott of the company and a general boycott of all Muslim-owned shops and businesses in Myanmar.[539] This has impacted on the company's ability to obtain tower sites in some areas.

Moreover, building on widespread anti-Muslim sentiment, some Buddhist leaders called on the Government to enact legislation to "*protect*" Buddhism. There are three laws in Parliament restricting the following: religious conversion to non-Buddhist religions; inter-faith marriage; population; and polygamy. The *Population Control Healthcare Bill* was passed by Parliament in April 2015. Parliament enacted the Buddhist *Women's Special Marriage Act* in July 2015. This law requires Buddhist women (but not men) to seek permission from the authorities to marry a non-Buddhist man.[540] International human rights organisations have noted that the *Population Control Healthcare Bill* may be used selectively against certain ethnic and religious minorities as there is no non-coercion or discrimination clause in the bill.[541]

Other faiths

People of other faiths also face discrimination and marginalisation. Christians comprise a small minority in the country, but most Chin and Kachin ethnic groups are Christian, with smaller numbers of Karen and Karenni Christians. Christians, like other members of minority religions, are generally not promoted to senior positions within the civil service or military. Ethnic minority Christians face restrictions on their religious freedom, including

[534] USAID, "Burma - Complex Emergency Fact Sheet #1, Fiscal Year (Fy) 2015" (6 Feb 2015).
[535] Brief Overview of the current human rights situation in Northern Arakan/Rakhine State, Myanmar, February – July 2014, Arakan Project, on file with IHRB.
[536] The White Cards expired on 31 March 2015. International Crisis Group, "CrisisWatch No 139" (2 March 2015), pg 12.
[537] Myanmar Times, "Former white card holders cut from Rakhine voter lists" (24 June 2015).
[538] ICG, The Dark Side of Transition: Violence Against Muslims in Myanmar" (Oct 2013).
[539] Nationalists call for Ooredoo boycott, Myanmar Times, 6 June 2014,
[540] The Irrawaddy, "Union Parliament Passes 'Interfaith Marriage Bill" (18 July 2015).
[541] See Amnesty International and International Commission of Jurists, "Myanmar: scrap 'race and religion laws' that could fuel discrimination and violence" (3 March 2015); Report of the Special Rapporteur on the situation of human rights in Myanmar, Yanghee Lee, Advance Unedited Edition, A/HRC/28/72, p 9-10, 9 March 2015; and "Burma's Population Control Bill Threatens Maternal Health Program", Physicians for Human Rights, 22 April 2015, *Population Control Healthcare Bill*.

limitations on building places of worship and destruction of religious venues and artefacts. These abuses are particularly acute in the context of the armed conflict in Kachin and northern Shan States.[542]

Women

Myanmar acceded to the *UN Convention against All Forms of Discrimination against Women* (CEDAW) in July 1997. The 2008 *Myanmar Constitution* does not include an effective constitutional guarantee of substantive equality[543] nor in practice do women receive equal pay for work of equal value.[544] Although the law guarantees equality between men and women, enforcement is weak and women are under-represented in Government and in most traditionally male occupations. In order to address some of these issues, in October 2013 the Government launched a 10 year action plan for the advancement of women.[545] The ADB and the UN have supported the Government in carrying out a Gender Status Analysis that provides a detailed assessment of the status of women in the country; the results were announced during January 2015.[546]

Women can be particularly at risk of negative impacts because they have fewer livelihood options than men, due to social status, family and cultural roles and expectations, and lower literacy levels,[547] and as a result, are disproportionally affected by poverty.[548] While the 2014 census reported an overall female literacy rate of 86.9%,[549] girls are often not able to attend school, particularly in remote mountainous border regions, which means that women are on the whole are less educated, leading to a lower literacy rate. Without access to education, women cannot access the job market, remain in low paid positions and are more prone to exploitation.

Sexual violence against women in the context of internal armed conflict in Myanmar has been reported for many years.[550] However an October 2014 report by the Gender Equality Network discussed violence against women in non-conflict situations, such as intimate partner violence, including marital rape, and sexual assault and harassment outside the home. The report recommended that companies implement policies to address and effectively respond to sexual harassment and violence in the workplace.[551]

Women's organisations in Myanmar speak out on a range of issues, including on the impact of business operations.[552] Article 19 has published a report, 'Censored Gender',

---

[542] United States Commission on International Religious Freedom, "2013 Annual Report" (2013), pg 22-25.
[543] Article 350 guarantees that women have the enforceable right to the "same rights and salaries" as that received by men "in respect of similar work." The use of the term "similar work" will not achieve the same equalities outcome as the principle of equal pay for work of equal value used in CEDAW. Myanmar Legal Framework Background Paper for IHRB, p 83, on file with IHRB.
[544] UNFPA Myanmar, "The 100th International Women's Day celebrated in Yangon, Myanmar" (8 Mar. 2011).
[545] UNDP,"Women's National Strategic Plan for Women Advancement Released" (4 October 2013).
[546] UNFPA, "Myanmar's Gender Status Analysis gets the Go-ahead" (18 January 2015).
[547] The Republic of the Union of Myanmar, "2014 Myanmar Population and Housing Census, Census Report Volume 2-A" (May 2015). pg. 37 on literacy ratios: male 92.6%, female 86.9%
[548] US Department of State, "Burma 2013 Human Rights report" .
[549] The Republic of the Union of Myanmar, "2014 Myanmar Population and Housing Census, Census Report Volume 2-A" (May 2015).
[550] UN General Assembly, "Report of the Special Rapporteur on the situation of human rights in Myanmar, Yanghee Lee" A/HRC/28/72 (9 March 2015), para 35.
[551] Gender Equality Network "Behind the Silence: Violence against women and their resilience in Myanmar" (October 2014).
[552] The Tavoyan (Dawei) Women's Union reported in February 2015 that women who protested about damage to livelihoods and the environment caused the Dawei Special Economic Zone and related projects in

examining how the right to freedom of expression and information applies to women in Myanmar and what gender-based violence is experienced by women as a result of what they say.[553] Some women's organisations campaigning against discrimination against women have received anonymous death threats via Facebook and their mobile phones.[554]

Other women's organisations are focussing on the gap between men and women working in the ICT sector. The founder of 'Geek Girls', a women in technology community in Myanmar, noted that 60% of the students at computer universities are female, but that women are lagging behind men in employment in the ICT sector, including in start-ups.[555]

Children

The Myanmar Government ratified the *International Convention on the Rights of the Child* (CRC) in 1991, and acceded to the *CRC Optional Protocol on the Sale of Children, Child Prostitution, and Child Sexual Abuse Images* in January 2012[556] and *ILO Convention No. 182 on the Worst Forms of Child Labour* in December 2013. Nonetheless Myanmar law diverges from the CRC in some significant areas. For example, the provisions of the *1993 Child* Law define a child as becoming an adult at 16 rather than 18 years, and sets the minimum age of criminal responsibility at seven years old. Although the Government has said that it will reform the law to bring it into line with the CRC, this has not yet occurred.

When discussing potential private sector impacts on children, the usual and often exclusive focus of companies is on child labour. However, ICTs can have a wider set of impacts on children, as a consequence of their physical and cognitive immaturity and vulnerability to exploitation. There is an increasing range of tools regarding children available to assist companies in identifying and understanding potential impacts on children.[557]

---

the southeast of the country also experienced harassment. Tavoyan Women's Union "Women activists facing harassment by proponents of the Dawei Special Economic Zone" (25 February 2015).
[553] 'Censored gender: women's right to freedom of expression in Myanmar' Article 19, June 2015
[554] See The Irrawaddy, "We Will Not Back Down" (19 June 2014).
[555] The Irrawaddy, "In Myanmar, Men are Leading the ICT Industry and "omen are Lagging" (8 May 2015).
[556] UN Treaty Collection
[557] UNICEF and the Danish Institute for Human Rights, "Children's Rights in Impact Assessments - A guide for integrating children's rights into impact assessments and taking action for children" (2013).

Child Labour

The 2008 Constitution reaffirms the State's responsibility to provide free basic education and health care for children.[558] The majority of children attend primary school, but the net completion rate is only 54%. Of these, only 58% go on to secondary school. [559] Due to widespread poverty and the unstable economic situation, many children drop out of school and work for low pay to help earn money for their families.[560]

Child labour is widespread and visible throughout Myanmar in various sectors (see census data in Chapter 4.6 on Labour). Children also end up as beggars on the streets, bus and railway stations and at tourist attractions. One survey found that one third of child labourers worked as street vendors.[561] The Government is working with the ILO and UNICEF to reform laws and end the worst forms of child labour. The minimum age for the employment of children is set at 13 years, which is in line with international standards for light work, but not in line with the international standard of 15 years for regular work.[562] The 1993 *Child Law* classifies children between the age of 14 and 17 as youths, and allows them to engage in "*light duties*". However, the term "*light duties*" is not defined.[563] Children are frequently victims of economic exploitation, as employers generally pay them less despite their high contribution of labour.[564]

Child Sexual Abuse Images Online

The increasing use of ICTs to distribute and access child abuse images[565] has given rise to numerous global coalitions and initiatives to identify and protect child victims and disrupt posting of and access to such images.[566] Distribution and accessing child abuse images are violations of children's rights and are a crime under international law. As noted by one of the leading NGOs working on disrupting the availability of child sexual abuse content hosted anywhere in the world, many legitimate online services are misused by those wishing to distribute child sexual abuse imagery.[567] Given the relatively low penetration of ICTs in Myanmar to date,[568] this has not been a major concern for children protection groups, but this is changing as the country opens further.[569]

---

[558] Ibid, pg. 4-5
[559] UNICEF, "Situation Analysis Myanmar" (July 2012) pg. 76 and 83.
[560] Democracy for Burma, "Child labour continues in Burma" (4 February 2011).
[561] UNICEF, "Situation Analysis of Children" (2012), p 116.
[562] Freedom House, "The Global State of Workers' Rights – Burma" (31 August 2010).
[563] US Department of State, "2013 Country reports on Human Rights practices, Burma 2013 Human Rights report" (2013).
[564] Child Rights Forum of Burma, "CRC Shadow Report Burma" (29 April 2011).
[565] A note on terminology: although the Optional Protocol to the UN Convention on the Rights of the Child uses what was the common term at the time to protocol was adopted "child pornography", the terminology has shifted to using the term "child abuse images" in order to convey more cleary the concept that any involvement with such images is a crime.
[566] See for example: European Commission, "A Global Alliance against Child Sexual Abuse Online" (last accessed August 2015).
[567] Internet Watch Foundation, "New tactics mean 137% increase in identified child sexual abuse imagery" (13 April 2015)
[568] See for example UNICEF, "Situation Analysis Myanmar" (July 2012), which highlighted many other existing child protection concerns in the country, but as of the 2012 date, there would have been little significant data or practice available about online exploitation. See also, Myanmar Centre for Responsible Business,

Under Section 66 of Myanmar's *Child Law*, the production or resale of child sexual abuse images can result in maximum fine of 10,000 MMK and a two-year prison sentence.[570] The use of a computer to sell, let to hire, distribute, publically exhibit, or put into circulation obscene objects is criminalised[571] under the Myanmar *Penal Code*, including for legal persons.[572] However, Myanmar does not have explicit provisions requiring Internet Service Providers (ISPs) to report suspected child sexual abuse images to law enforcement or other agencies upon discovering suspected child sexual abuse images or other types of child abuse/child sexual exploitation circumstances on their network.[573]

Ethnic Minorities

Ethnicity is a complex, contested and politically sensitive issue. Ethnic groups have long believed that the Government manipulates ethnic categories for political purposes.[574] (See Chapter 4.10 on Conflict and Security for information about ethnic minority armed groups). Myanmar's ethnic minorities make up an estimated 30 – 40% of the population, and ethnic states occupy some 57% of the total land area along most of the country's international borders.[575] Political boundaries in Myanmar are to some extent organised according to ethnic demographics. The seven states are named after seven large ethnic minority groups – namely, Kachin, Kayah, Kayin, Chin, Mon, Rakhine, and Shan States. Although the Bamar do not have a specific state named after them, they are the dominant ethnic group living in the country, especially in the seven Regions (Sagaing, Magwe, Tanintharyi, Mandalay, Yangon, Ayeyarwady, and Bago). There are also six self-administered areas that are part of Regions or States, each named after the minority national race that forms the majority in the relevant area (Naga, Danu, Pa-O, Palaung, Kokang and Wa Self-Administered Areas)[576].

The term 'Indigenous Peoples' is not widely understood in Myanmar, nor generally used. The 2008 *Myanmar Constitution* makes no reference to ethnic minorities or indigenous peoples, instead using the term "*national races*". However, "*national races*" is not defined, and is generally interpreted by applying the 1982 *Myanmar Citizenship Law*, which defines 135 national races in its 1983 *Procedures*.[577] Under the *Myanmar Citizenship Law*, nationals of Myanmar include the "*Kachin, Kayah, Karen, Chin, Bamar, Mon, Rakhine or Shan and ethnic groups as have settled in any of the territories included within the State as their permanent home from a period anterior to 1185 B.E., 1823 A.D.*"[578]

Article 22 of the Constitution, provides for *"(i) development of language, literature, fine arts and culture of the national races; and (ii) promotion of solidarity, mutual amity and respect*

"Myanmar Tourism Sector Wide Impact Assessment" that highlighted rising concern and attention to the exploitation of children in tourism, pg. 157-158.
[569] See for example, UNCEF, "Child Safety Online – Global Challenges and Strategies" (2011).
[570] Burma Library, "SLORC's Child Report – 4" (26 January 1997).
[571] *Myanmar Penal Code*, Section 292.
[572] Ibid, Section 11.
[573] International Centre for Missing and Exploited Children, "Myanmar Country Report" (2014).
[574] International Crisis Group, "Myanmar Conflict Alert: A Risky Census" (Feb. 2014).
[575] Transnational Institute/Burma Centrum Netherlands, "Access Denied: Land Rights and Ethnic Conflict in Burma", (May 2013).
[576] *Myanmar Constitution* (2008), Article 56.
[577] See: Burma Library, "Burma Citizenship Law of 1982" (last accessed August 2015).
[578] *Myanmar Citizenship Law*, Article 3.

and mutual assistance among the national races; and promotion of socio-economic development including education, health, economy, transport and communication, of less-developed national races".

Almost all Rohingya are denied citizenship under the 1982 *Myanmar Citizenship Law,* either because they do not meet its stringent and discriminatory citizenship requirements, or where they do, because they lack the documentary evidence required. People of Chinese, Indian or Nepali heritage are mostly denied full citizenship under this law because they do not automatically qualify under "*national races*".

The 2014 national census used the 135 categories of national races, with people required to check one of them, or indicate "*other*"; there was no option to indicate the frequent mixed heritage of many residents. This 135 national races categorisation is strongly contested by ethnic minorities, as they believe it does not accurately represent their true ethnicity and also that the Government, comprised primarily of ethnic Bamar, is using this to lower the real number of each broad ethnic group. A last minute Government decision prevented those Muslims in Rakhine State identifying as Rohingya to write in "*Rohingya*" as their ethnic group during the census process.[579] The Government has not yet released 2014 census ethnicity data.

The Protection of the Rights of National Races Law[580] enacted on 24 February 2015 gives further effect to Article 22 of the 2008 Constitution. Article 3 includes the purposes of the law: "*(e) to aim for the socio-economic development of less-developed national races including education, health, economics and transportation*." While Article 3 of the law provides for "*access to equal citizenship rights for all ethnic groups*", and for "*ethnic groups to have full access to rights enshrined in the Constitution*", it does not explicitly protect ethnic minorities against discrimination. The law states that no one can behave with intent to incite hatred, animosity and disunity among "*national races*" and that ethnic rights and entitlements cannot be restricted without a sound reason.

The 2015 Law establishes a Minister for National Races to be appointed by the president with the approval of the union Hluttaw. This has not yet taken place. In article 9 the Ministry's duties and mandate includes: "(e) *carry out all round development activities including education, health, economics and transportation of less developed national races for their socio-economic development and article*;" and (j) "*carry out activities to develop, maintain, protect and improve language, literature, arts, culture and traditions of minority and ethnics' tribes in danger of extinction*". It is not yet clear whether this will extend to supporting the development of online content in ethnic minority languages.

[579] See International Crisis Group, "Counting the Costs: Myanmar's Problematic Census" (15 May 2014).
[580] Available at: http://www.pyithuhluttaw.gov.mm/lawdatabase/?q=my/law/431 (Burmese only).

People Living With Disabilities

The 2014 Census reported a disability rate of 4.6% of the total population.[581] A 2010 study noted that people with disabilities in Myanmar suffer from widespread discrimination and exclusion within their communities, families, and from society as a whole. Disabled children and women were identified as the most vulnerable.[582] Moreover, Myanmar activists have reported that people living with disabilities are not adequately protected by law and have called for stronger protection for this population, as they are at risk of abuse.[583] There is a severe lack of education for people living with disabilities; a Myanmar Government study reported that almost 50% of disabled people received no education whatsoever. The survey also reported that 85% of disabled people were unemployed.[584] There have been very few employment training programs for people with disabilities, and there is a need for more vocational training and employment, supported by funding.

Myanmar acceded to the *International Convention on the Rights of Persons with Disabilities* (CRPD) in December 2011.[585] The Ministry of Social Welfare is the Myanmar Government entity responsible for people with disabilities (PWD) [586]. A Disability Rights Law 30/2015, drafted with input from disabilities advocacy organisations, was adopted in June 2015[587]. This provides for the creation of a National Committee for Disability Rights with extensive government and NGO participation (but not business). The Committee will address issues such as access to employment, discrimination and vocational training. Tax relief will be available for goods produced by PWDs, and for organizations or private business *'that employ more than the designated quota of PWDs'*.

No further details are given about the envisaged quota system, which it appears will be defined by the National Committee. The Law sets out the responsibilities of employers to obey and implement the policy of National Committee for creation of job and training opportunities for PWDs; employ PWDs (including those who are registered at township Labour Offices) in suitable workplace in accordance with the quota system. Where the employer is unable for whatever reason to employ PWDs, they shall contribute to a fund for PWD rights according to a rate to be laid down. The Ministry of Social Welfare is expected to begin work on bye-laws in late 2015.

The Myanmar Centre for Responsible Business (MCRB), along with the Deaf Resources Centre, has published a bilingual Guide for companies wishing to integrate people with disabilities into their Corporate Social Responsibility (CSR) policies, increase the level and quality of employment for people with disabilities, and contribute to the improvement of products and services for people with disabilities.[588]

---

[581] The report listed four types of disability: walking, seeing, hearing, intellectual/mental. The Republic of the Union of Myanmar, "2014 Myanmar Population and Housing Census, Census Report Volume 2-A" (May 2015).
[582] Salai Vanni Bawi, "Understanding the Challenges of Disability in Myanmar" (2012).
[583] Myanmar Times, "Activists call for stronger laws to protect Myanmar's disabled" (21 January 2013).
[584] The Irrawaddy, "In Burma, Children with Disabilities Struggle to Access Schools" (5 November 2013).
[585] United Nations Treaty Collection.
[586] Myanmar Ministry of Social Welfare.
[587] http://www.pyithuhluttaw.gov.mm/?q=download/file/fid/5478 only availability in Burmese
[588] MCRB and Deaf Resources Centre "Corporate Social Responsibility and Disability (CSR-D)" (Aug 2014).

Lesbian, Gay, Bisexual and Transgendered (LGBT) People

Article 377 of the *Penal Code*, based on British colonial law, criminalises any activity that the Myanmar authorities decide constitutes "*carnal intercourse against the order of nature*".[589] The LGBT Rights Network in Myanmar has called for the abolition of this article, which can be used against people in same-sex relationships. Although greater freedom has led to greater visibility for LGBT activists, this has meant that they are now exposed to more abuse. LGBT activists have reported widespread discrimination, and general societal lack of support.[590] The US State Department's 2014 Annual Human Rights Report states that LGBT people in Myanmar face discrimination in employment, including denial of promotions and dismissal. Openly gay men and lesbians also report limited opportunities for work and harassment by the police.[591] LGBT activists have reported online abuse; homophobic groups shared photos of some prominent LGBT activists. After the wedding of two gay men, there was a spike in such abuse online, including death threats against all gay people. Online abuse against the LGBT community is a serious problem in Myanmar and ICT companies should be aware of the potential for such abuse.

B. Field Research Findings

Religious Communities

Human Rights Implicated: Right to non-discrimination

Field Assessment Findings

- As noted in Chapter 4.6 on Labour, **racial and religious tensions were observed, mainly where communities identified the company or its workers as Muslim:**
  - Researchers heard of several incidents in which subcontractors of a company from a majority Muslim country were disturbed in their work by communities protesting the company's presence in their area.
  - Workers were denied accommodation due to working for a Muslim company.
- Communities threw stones at cars carrying workers of companies that were perceived to be owned by Muslims.

Gender

Human Rights Implicated: Right to non-discrimination

Field Assessment Findings

- With respect to the acquisition or leasing of land for tower or cable sites, in principle, there is no legal impediment to **providing payment for land or lease compensation to women or women-headed households**. Nonetheless, households are registered in the husband's name and therefore in general compensation was handed over to the male household head. However, widows or single mothers would also be able to obtain compensation same way as male headed households.

[589] Lawyers' Collective, "LGBT Section 377" (23 November 2010). This *Myanmar Penal Code* is still used by many countries formerly ruled by the British, including India, Malaysia, and Myanmar.
[590] The Irrawaddy "LGBT Groups Call for Burma's Penal Code to Be Amended" (29 November 2013).
[591] US State Department, "Burma 2013 Human Rights Report" (2013) pg. 40 – 41.

- As noted in Chapter 4.6 on Labour, it was very unusual for **any women to work on tower construction**.
  - This was often justified on the grounds it was unsafe for them due to night work and the distances between the site and their village/ accommodation.
  - Where women were able to work on tower construction sites, they were only allowed to do certain manual tasks, such as backfilling or moving materials.
- **Perceptions of women working in the ICT sector were mixed** amongst interviewees. Given traditional cultural norms in Myanmar, many indicated women and girls should not work and should stay at home to support their families. However, just as many indicated that female workers were excelling at programming and that there were more female students than male students at computer universities, including at masters level.
- Some stakeholders suggested that in order to protect women against such online harassment or hate speech, the **draft Anti-Violence Against Women Law** should include provisions addressing these problems.

Children & Young People

Human Rights Implicated: Rights of the child

Field Assessment Findings

- Field researchers heard **repeated appeals for better curricula and facilities within schools and universities, especially regarding technology and engineering:**
  - Myanmar universities and the ICT industry were seen as disconnected; many students felt the university curriculum needed to be redesigned in consultation with industry.
  - The computer and tech university curriculum was seen as 10 years behind, for example teaching students Visual Basic programming language (created in 1991) rather than the more recent successor visual basic.NET (created in 2002). Companies seeking to hire qualified local staff noted skill gaps, and low job-readiness skills as limiting factors.
  - Primary schools have not yet integrated ICT education into curricula, leading to a lack of basic skills needed to successfully pursue university programmes on ICT amongst the majority of Myanmar young people
- **Numerous cases of the negative impacts of over-use or misuse of the Internet were shared with researchers**, particularly by concerned parents. This was mainly ascribed to the sudden exposure to the Internet without any education on the safe or balanced use of technology. As in many other parts of the world, **parents expressed concern about children** becoming 'addicted' to computer games either offline or online. In some cases this has led to children dropping out of school.
- As noted in Chapter 4.6 on Labour, occasional practices of reviewing identification to verify workers' age were reported in fibre cable installation projects, but many more instances of lack of identification cards or documents were described to researchers, indicating a **general lack of basic measures to prevent underage workers in fibre and cable installation in particular**.
  - Fibre cable line workers often had to travel long distances from their homes in order to take up work. Due to lack of childcare, and shifting worksites, they would bring children with them. As a consequence **children were regularly left waiting in the worker camps during the 10 hour shift periods**.

Myanmar Good Practice Examples:

- One company has reported that their Code of Conduct covers human rights and also has a Myanmar-specific statement on human rights due diligence requirements. They have established a community outreach program with State Liaison Officers to act as a link between ethnic groups and the company, and a local hotline to which people may report grievances related to sustainability issues.[592]

C. Groups At Risk: Recommendations for ICT Companies

Understanding and Addressing Differentiated Impacts of Projects

- **Understand the Myanmar context:** Myanmar has a very diverse population in a complex and often conflict-ridden environment. Myanmar legal standards often fall below international legal standards to protect groups at risk. The groups at risk are often (at best) neglected parts of the population and at worst, subject to persecution by the Government or others. In these situations, in addition to international guidance on engagement and employment or contractual arrangements with groups at risk, experts on the specific vulnerable group in question should be consulted.
- **Identify and engage:** A first step in understanding what potential impact a project or services may have on groups at risk is to identify which vulnerable groups may be in the potential workforce and surrounding community as part of the company's due diligence process. The ICT value chain is spread across the country and their workers and stakeholders will vary in different locations. This assessment may require additional specialist sociological or anthropological expertise and methods to identify, locate and engage individuals or groups at risk of abuse and marginalisation. Engagement may often need to be done separately, and sometimes discretely.
- **Ensure assessments and prevention are differentiated:** The objective of an assessment is to better understand how impacts may affect each potential group at risk, and in particular, to understand who could experience adverse impacts from the proposed project or service more severely than others. Disaggregated data and community consultations/focus groups will be needed to identify, assess and discuss potential impacts. Differentiated prevention or mitigation measures may be required to address the greater severity of impacts. Monitoring should track impacts on individuals or groups on a disaggregated basis.
  - Groups at risk should also be able to benefit from ICT sector equally with others. This too may require distinct measures. For example, if job training is offered, there may be a need for specialised or separate training provided for individuals from groups at risk who face exclusion from the dominant group, e.g. people living with disabilities.
- **Consider the potential exposure of users at risk:** As noted elsewhere (See in particular Chapter 4.1 on Freedom of Expression and Chapter 4.4 on Surveillance and Chapter 4.2 on Hate Speech), some of those groups highlighted in this Chapter are subject to specific risks within Myanmar. ICT companies who provide services for or affecting these groups (such as by hosting online content) should consider these vulnerabilities in advance of offering services. They should consider what steps can be taken to modify policies, procedures or services to avoid or minimise negative impacts on them, which might derive from hate speech, bullying or unlawful surveillance.

[592] See further: Telenor, "Response by Telenor: Myanmar Foreign Investment Tracking Project", Business & Human Rights Resource Centre (last accessed September 2015).

- **Address child safety online**: As Myanmar does not have specific laws covering child safety online and is unlikely to be able to prioritise these issues, given the wide range of other child protection challenges in the country, it will fall to companies to take action to protect young users and to disrupt the use of their services to transmit child abuse images. Telecommunications operators and web based services, as well as software companies, need to consider the range of potentially severe impacts on children that can occur through different forms of violence and exploitation. For example, the online sale and trading of child abuse images is considered a crime in most jurisdictions and prohibited under international human rights law. Other negative impacts arise from broader child safety issues online, such as 'cyber bullying', 'grooming', the illegal sale of products such as alcohol or tobacco to children, or graphic content encouraging self-harm. Companies should report clearly abusive images or behaviours promptly to law enforcement authorities once they become aware of them. Beyond this, there is a range of approaches that companies should draw on, including:
  - making it clear how users can report abusive images or behaviour such as bullying
  - training moderators of online forums and services for children to help identify and respond to concerning or suspicious behaviour
  - implementing effective age and identity verification mechanisms at the level of individual users
  - implementing appropriately heightened security measures for personal information that has been collected from children (including any location-related information, which can pose particular risks to children)
  - seeking parental consent before using or disclosing information collected from children;
  - considering any unintended consequences of decisions on child safety (for example, posting information about unaccompanied children on privately-run, post-disaster family reunification websites), and
  - engaging with external child safety and children's rights experts, including relevant civil society organisations and the Government, to provide on-going feedback and guidance on the company's approaches.[593]

Business Leadership

- **Model equal opportunity:** Addressing entrenched discrimination demands a change in societal attitudes, which often requires prompts from many directions to tip the balance towards broader acceptance. These can include messages from the political leadership – the President's office has repeatedly called for building an "*inclusive and sustainable*" Myanmar – as well as changes in law and changes in peer countries. However, changes can also start with the private sector modelling equal opportunity and demonstrating the benefits. This is an important role that businesses of all sizes in the ICT value chain can play, through leadership messages and by creating workplaces that are not only visibly free of discrimination but also moving towards equal opportunity for the groups at risk of marginalisation noted above.

[593] See for example: ITU et al, "Guidelines on Child Protection Online"; GSMA, "The Mobile Alliance against Child Sexual Abuse Content", European Commission, "Global Alliance on Child Sexual Abuse Online" (last accessed August 2015). The ASEAN Commission on the Promotion and Protectin of the Rights of Women and Children has not made online protection a priority in its "Work Plan (2012-2016) and Rules of Procedures (ROP)" (2012).

- **Highlight impacts on investment climate:** Societal discrimination and exclusion are not unique to Myanmar. However, if discrimination and exclusion becomes more entrenched and overt, it will undermine ongoing political and economic reforms. Businesses, collectively or individually, should highlight how the negative impacts of discrimination and inter-communal violence, and an inadequate response from the Government on protecting those at risk, can harm the investment climate.
- **Design ICTs for vulnerability and accountability:** As outlined in Chapter 3 on sector-level impacts, there are more opportunities for positive impact from the ICT sector than potentially any other industry developing within Myanmar's fast moving landscape. The nature of the ICT sector – able to bridge long distances affordably and in real time – positions it to combat exclusion and vulnerability. For example, ICT can increase access to doctors and medical services for the elderly, disabled or displaced who are in desperate need of healthcare but often unable to travel or afford it; provide people with disabilities with accessible online employment opportunities; and offer hotlines for groups at risk.

D. Relevant International Standards and Guidance on Groups at Risk

Relevant International Standards:

- IFC Performance Standard 2 and Guidance Note – Labour and Working Conditions
- ILO, Discrimination (Employment and Occupation) Convention (No. 111)
- UN Convention on the Elimination of Discrimination Against Women
- UN Convention on the Rights of Persons with Disabilities
- UN Convention on the Rights of the Child

Relevant Guidance:

- European Commission, "ICT Sector Guide on Implementing the UN Guiding Principles on Business & Human Rights"
- IFC, "Good Practice Note, Non-Discrimination and Equal Opportunity"
- ILO, "Working Conditions of Contract Workers in the Oil & Gas Industry"
- ILO, "Disability in the Workplace – Company Practices"
- CSR-D, "Guide on Corporate Social Responsibility and Disability" and in Burmese, MCRB and DRC, "Corporate Social Responsibility and Disability (CSR-D) – A Guide for Companies in Myanmar"
- UNICEF, UN Global Compact, Save the Children, "Children's Rights and Business Principles"
- UN Global Compact, "Women's Empowerment Principles"
- UN "Inter-Agency Handbook on Housing and Property Restitution for Refugees and Displaced Persons: Implementing the 'Pinheiro Principles'"

Chapter 4.9

Stakeholder Engagement & Grievance Mechanisms

4
4.9

Chapter 4.9

Stakeholder Engagement & Grievance Mechanisms

In this Chapter:

A. Context

Stakeholder consultation and engagement in Myanmar are complex for a number of reasons. Until recently people's rights to speak freely or assemble peacefully had been forcefully suppressed for five decades. As a result, many individuals are still reluctant, even fearful, about speaking out against the Government or military in particular. Ethnic diversity, and experience of armed conflict and inter-communal violence, have resulted in significantly different perspectives on the role of the Government and business which may be difficult for outsiders to access and understand. The ability to organise NGOs to address key concerns was extremely difficult until Cyclone Nargis in May 2008, when the authorities began to tolerate the participation of civil society in humanitarian work, although CSO leaders were also arrested and imprisoned at the time. The Government has historically placed itself as the main interface between companies and communities. This approach will take time to change, but is now beginning to happen.

The country has suffered and continues to suffer an accountability deficit that will take far longer to change, starting with changing mind-sets. At the highest level, reformers in the Government have indicated their willingness to be held accountable and have taken several significant steps to join international initiatives to begin to address both international and domestic concerns. These include joining the Extractive Industries Transparency Initiative (EITI),[594] and initiating its application to the Open Government Partnership (See Chapter 3 on Sector Impacts). Both of these initiatives require active

594 Myanmar EITI is based on a number of principles including transparency and accountability. EITI membership also requires that civil society are able to operate freely and "*are able to speak freely on transparency and natural resource governance issues, and ensure that the EITI contributes to public debate*." EITI, "Civil Society Protocol" (1 January 2015).

engagement of a civil society that is able to speak freely. The experience of getting them launched highlights the challenges ahead in changing mind-set at all levels of Government. Those changes are important for many reasons, not least because the more formal structures for citizens and others to hold Government to account – such as a functioning independent judicial system – are very weak and will take years to address. In the meantime, the highest levels of Government need to ensure that they are sending clear and consistent signals on the importance of accountability and transparency. This, and putting in place mechanisms like the E-Governance Master Plan, may help reduce the governance gap (See Chapter 3 on Sector Impacts).

Freedom of Expression

See Chapter 4.1

Freedom of Peaceful Assembly

In December 2011 Parliament enacted the *Law Relating to Peaceful Assembly and Peaceful Procession*, which permits peaceful assembly for the first time in several decades. However, prior permission from the Government (the Township Police) is still required for an assembly/procession of more than one person and the requirements for seeking such permission are unduly onerous. Article 18 of the law has often been used to target activists and human rights defenders, many of whom have been arrested and imprisoned under its provisions. It acted as a significant deterrent as it provided for up to one-year imprisonment for those who demonstrate without prior permission.[595] Parliament amended the law on 19 June 2014; new amendments now reportedly oblige the authorities to grant permission for peaceful demonstrations unless there are "valid reasons" not to do so, and punishment for failing to seek prior permission and holding a demonstration without such permission was reduced from one year to six months.[596] However, the amended law still provides for the arrest and imprisonment of peaceful protesters. Arrests and imprisonment of such activists increased throughout 2014 and the first half of 2015.

Protests, including against private sector projects, particularly those in the extractive industries, have been suppressed in the past, sometimes violently. The authorities continue to crack down on such protests, with participants arrested and sometimes subjected to beatings and other ill-treatment.[597]

[595] Pyidaungsu Hluttaw, *The Right to Peaceful Assembly and Peaceful Procession Act* (Dec. 2011). Requirements include an application form submitted at least five days in advance; the biographies of assembly leaders and speakers; the purpose, route, and content of chants; approximate number of attendees, amongst other things. See Chapter 3, 4.
[596] DVB, "Peaceful Assembly Bill passed, now awaits President's signature" (19 June 2014).
[597] Norwegian Council on Ethics, Pension Fund Global, "Recommendation on the exclusion of Daewoo International Corporation, Oil and Natural Gas Corporation Ltd., GAIL India and Korea Gas Corporation from the investment universe of the Government Pension Fund Global" (2012). See also the 2013 Recommendation concerning the post-construction phase of the project.

4
4.9

Freedom of Association

A network of civil society and community-based organisations is active at both the national and local levels, including many ethnic minority-based groups. In the aftermath of Cyclone Nargis, Myanmar CSOs greatly expanded and organised as they worked to help survivors. They have remained a significant positive force in the country and have been able to engage with the Government to some extent. Since 2011 Myanmar civil society groups have had more freedom to organise and have taken that opportunity to increase their activities to help people claim their rights, including those affecting local communities.

An early draft of the *Association Registration Law* required all groups to be formally registered, with severe penalties for failing to do so. CSOs raised this as a key concern, with the EITI CSO group asking for clarification before agreeing to participate in EITI. The law was adopted in July 2014 with this provision removed. It retains another provision of concern to CSOs, which requires groups who do decide to register to do so at township, state or national level, thereby potentially restricting their area of operation.[598] The website of the International Centre for Not-for-Profit Law (ICNL) provides information on laws relating to Myanmar civil society.[599]

Corruption

Myanmar ranks 156th out of 175th on Transparency International's Corruption Perception Index. In December 2012 the President announced that the Government would tackle pervasive corruption in its ranks,[600] and ratified the UN Convention against Corruption (UNCAC).[601] An Anti-Corruption Law was enacted on 7 August 2013 by the legislature although the President's Office submitted comments highlighting weaknesses and inconsistencies with UNCAC.[602] The law is to be implemented by the recently established Anti-Corruption Commission appointed in February 2014. The Commission comprises 15 members, five of who are appointed by the President, with another five each appointed by the speakers of both houses. However MPs have raised concerns that the Commission is not effective, noting in September 2014 that it had only dealt with three out of 533 cases.[603]

While it is encouraging that the Myanmar Government has acknowledged the problem of widespread corruption and begun to take steps to address the issue, it remains a major risk for companies investing in Myanmar. Given the home state anti-corruption laws that apply to many of the larger international ICT companies and the significant fines for violations, this will be an on-going issue, as it will take time for corruption to be

[598] DVB, "Activists relay worries of draft association law to parliament" (5 June 2014).
[599] ICNL, "NGO Law Monitor: Myanmar (Burma)" (accessed 25 July 2014).
[600] Third phase of reform tackles govt corruption, President says, *The Irrawaddy*, 26 December 2012.
[601] United Nations Convention against Corruption Signature and Ratification Status as of 2 April 2014, United Nations Office on Drugs and Crime (accessed 15 July 2014).
[602] The Republic of the Union of Myanmar President's Office, "Press Release on the Promulgation of Anti-Corruption Law" (8 August 2013). The Law incorporates provisions that are in certain respects narrower than those used in the Organization for Economic Co-operation and Development Convention on Combating Bribery of Foreign Public Officials in International Business Transactions (OECD Convention). The definition of "bribe" incorporated in the law is narrower than that used in the OECD Convention. Further, Myanmar's anti-corruption law does not include provisions that address accounting and record-keeping standards.
[603] The Irrawaddy, "MPs Voice Doubts Over Burma's Anti-Corruption Commission" (24 September 2014).

significantly reduced in all levels of the Myanmar Government. Speaking out publicly about tackling corruption is an important contribution businesses can make towards this.

Lack of Transparency

Interactions between the Government and the people of Myanmar have been marked by a lack of transparency on the part of the authorities, including about business operations. Recently the Government has begun to take limited steps to improve transparency through Government-controlled media and the President's and Ministry websites.[604] For example the Ministry of Labour, Employment, and Social Security publishes the text of recent laws and provides information about benefits.[605] However, there is currently no freedom of information (FoI) law in Myanmar. Civil society is advocating for FoI legislation, and the Open Myanmar Initiative (OMI), a consortium of CSOs, is conducting research and convening discussions on such a law.[606] Local government generally does not provide relevant information to communities about business operations in their areas, as revealed by SWIA field assessments in the ICT, tourism, and oil and gas sectors. (See Chapter 4.1 on Freedom of Expression).

Accountability: Judicial and Non-Judicial Mechanisms

The previous Government was characterised by a lack of accountability for human rights violations and violations of international humanitarian law. Those who dared complain about the authorities or companies were at risk of reprisals, including arrest, torture, and imprisonment. Since the reform process began in 2011, there has been a marked increase in calls by communities to provide redress for abuses, particularly around "land grabs" and labour rights. The Government's response has been at times contradictory, which may be partially explained by the different levels of Government involved in responses, at the Union and local levels. The President has repeatedly exhorted all levels of Government to be more accountable, but at the local level, and indeed in some Union Ministries, such accountability is still absent. The lack of clarity may also be due to tensions between reformers in the Myanmar Government and its more conservative elements.

Both the EITI and the Open Government Partnership include independent, third party checks on whether the Government is meeting its obligations to promote more open civil society that can hold the Government to account. This external, third party review can provide an important avenue for civil society to raise concerns.

Arrests of peaceful protestors increased during 2014, and in March 2015 police beat and arrested student demonstrators in Letpadan, Bago Region. The Myanmar National Human Rights Commission has called for prosecution of the security forces involved.[607] It is not known whether the government – which is currently prosecuting the beaten students – will follow up.

---

[604] See for example: Republic of the Union of Myanmar President's Office and Myanmar Ministry of Home Affairs.
[605] See: Myanmar Ministry of Labour, Employment and Social Security.
[606] Eleven Media, "Rights group pushing for freedom of information law" (last accessed August 2015).
[607] 'Rights Commission urges action against the police' Myanmar Times, 14 September 2015

With respect to the judiciary, reforming the rule of law in Myanmar has been a major focus of President U Thein Sein's administration. The Government's "*Framework for Economic and Social Reforms*" notes "*the lack of effectiveness and predictability of the judiciary*".[608] The judicial system is widely considered to be "*under-resourced, politically influenced and lacking in independence*".[609] However, reform will take a long time, and substantial resources – and not least – changes in attitude to the rule of law, starting from the bottom up, with attention to legal education. The legal education system has been eroded by decades of under-investment, and the legal profession greatly constrained by long-term political restrictions, leading to a major shortage of lawyers taking up cases.[610]

Judicial independence in Myanmar to date has been essentially non-existent,[611] with judges accustomed to acting "*as administrators rather than arbiters, basing decisions on state policy, instead of legal reasoning and the application of precedent*".[612] While there are basic principles of separation of powers provided by the Constitution, it is not complete. A 2013 report by the parliamentary Rule of Law and Stability Committee, led by Daw Aung San Suu Kyi, found "*continued intervention by administrative officials in the judicial system*".[613] This indicates that structural changes will be required to put in place a rigorous separation of powers. There is no Ministry of Justice.

Systemic corruption in the administration of justice is a major concern, manifesting itself through bribes, delays, and obstructions,[614] with a widespread local perception that the courts in Myanmar are corrupt and unfair.[615] As a result, many would "*[resort] instead to local-level dispute resolution mechanisms they perceive to be more reliable, accessible and affordable*".[616] These local-level mechanisms generally involve village leaders and/or elders' councils. Although the village leader has an obligation to inform the police about serious crimes, smaller issues and petty crimes can be settled by the village leader and/or the elders' council, a small group of respected men in a village. If one party to the problem does not agree with the solution reached, they can take the matter to the township level, but this rarely happens because it is seen as being too expensive, considering both the administrative legal costs and bribes that would have to be paid.
There is currently little in the form of a legal aid system in Myanmar, making it impossible for many to afford the time and cost commitments of using the court system. In conflict areas, the issue may be taken to the administration of the controlling armed group.[617] In addition to the courts, other bodies responsible for the administration of justice, including

[608] Government of Myanmar, "Framework for Economic and Social Reform - Policy Priorities for 2012-2015 towards the Long-Term Goals of the National Comprehensive Development Plan (FESR)" (January 2013), para 116
[609] OECD, "OECD Investment Policy Reviews: Myanmar 2014" (March 2014), pg. 27.
[610] See: International Commission of Jurists (ICJ), "Right to Counsel: The Independence of Lawyers in Myanmar", (Dec 2013)
[611] Human Rights Resource Centre, "Rule of Law for Human Rights in ASEAN: A Baseline Study" (May 2011), pg. 163, citing Asian Legal Resource Centre, Amnesty International, "Myanmar: No Law At All – Human Rights Violations under Military Rule" (1992).
[612] International Bar Association's Human Rights Institute, "The Rule of Law in Myanmar: Challenges and Prospects" (Dec 2012), pg. 56.
[613] The Irrawaddy, "Interference in Judicial System Harming Burmese People: Lawmakers" (14 August 2013).
[614] ICJ, "Right to Counsel: The Independence of Lawyers in Myanmar", (Dec 2013)
[615] See: USIP, "Burma/Myanmar Rule of Law Trip Report" (June 2013), pg. 5 and 34.
[616] Ibid, pg. 5.
[617] Ibid.

the police, lack the training and capacity to enforce the rule of law (though the EU has been providing training to improve the human rights performance of Myanmar's police).[618]

The Government has also taken a number of actions to provide non-judicial grievance mechanisms to the public in the absence of a fully functioning judiciary (see Table 40 below). However, these mechanisms are already overloaded with complaints and hindered by limited mandates. Since the reform process began, these committees and the Myanmar National Human Rights Commission have received thousands of complaints from the public about abuses at the hands of the Government and military, but, as noted above, many of these people still await a resolution to their problems.

Many businesses commonly seek to incorporate safeguards into their investment contracts by ensuring access to international – rather than domestic – arbitration tribunals in the event of an investment dispute.[619] Myanmar acceded to the 1958 New York Convention on the Recognition and Enforcement of Arbitral Awards in April 2013, which entered into force July 2013.[620] This solidifies the ability of foreign investors to submit disputes with Myanmar Government and commercial partners to international arbitration. The Myanmar legislature is now reportedly considering a new law based on the 1985 *UNCITRAL Model Law on International Commercial Arbitration* to replace the 1944 Arbitration Act, which would enable Myanmar courts to recognise and enforce international arbitral awards.[621]

An equivalent assurance of access to remedies for most Myanmar people affected by private sector operations is still a practical impossibility. Accountability in Myanmar is a new phenomenon and one that will take time to become established. Given the inefficiencies and acknowledged corruption in the judiciary and the inability of even the ad hoc commissions to resolve complaints, there is a clear lack of access to effective avenues for individuals and communities to express their grievances, engage with responsible parties in the Government or to seek redress if harms have occurred – especially at the local level.

Table 40: Existing Non-Judicial Grievance Mechanisms in Myanmar

- Daw Aung San Suu Kyi was appointed to head up a new **parliamentary Rule of Law and Stability Committee** formed in August 2012 to serve as a mechanism for the general public to lodge complaints about Government departments. In one month it received over 10,000 complaint letters regarding courts within the Yangon Division alone.[622]
- The **President's Office opened a public access portal** for people to submit opinions and complaints directly to the President.[623]
- A non-judicial **labour dispute settlement system** to resolve disputes between

[618] EU Delegation to Myanmar, "EU Crowd Management Training Supports Reform of Myanmar Police Force" (Feb 2014).
[619] More recently, the EU and Myanmar have begun discussions on an investor-state dispute settlement mechanism with Myanmar. See for example: Herbert Smith Freehills, "Myanmar and the European Union to enter into an investment protection agreement" (13 March 2014).
[620] *New York Convention on the Recognition of Foreign Arbitral Awards* (1958) (last accessed August 2015).
[621] Singapore International Arbitration Blog, "Draft Arbitration Bill in Myanmar" (June 2014).
[622] Regarding the various bodies noted, see further: Hnin Wut Yee, "Business & Human Rights in ASEAN – A baseline study: Myanmar chapter" (April 2013).
[623] Government of Myanmar, "FESR - Policy Priorities for 2012-2015 towards the Long-Term Goals of the National Comprehensive Development Plan" (January 2013), para 114.

employers and workers is in place, involving requiring workplaces to establish Workplace Coordination Committees, but implementation is still weak due to lack of adequate knowledge about the newly enacted labour laws.

- There are a number of mechanisms to hear land disputes, including a **parliamentary committee on land confiscation inquiry**, but without a mandate to give binding decisions. (See Chapter 4.7 on Land)
- The **Myanmar National Human Rights Commission** (MNHRC) was established in September 2011, but the *MNHRC Law* was only enacted on 28 March 2014. The MNHRC has a broad mandate of promoting and monitoring compliance with human rights. It is empowered to investigate complaints and contact the concerned person, company or Government department and can recommend action. It can also make its recommendations public. It can undertake inquiries and will prepare an annual report to the President and Parliament. It is also mandated to consult different stakeholders including CSOs. The President selects members after proposals by a selection board. While the law provides that proposed members should have expertise or knowledge in different areas relevant to human rights including from civil society, it does not guarantee pluralism, nor a total independence from the Executive, in accordance with the Paris Principles.[624] It received over 1700 complaints in its first 6 months of operation, a majority of which involved land grabs.
- The **ILO and Myanmar Government have agreed a complaints mechanism** to allow victims of forced labour an opportunity to seek redress/remedies from Government authorities in full confidence that no retaliatory action will be taken against them.[625] The October 2013 report by the Myanmar Liaison Officer notes an increasing number of complaints about forced labour in association with land confiscation, with people either losing their livelihoods completely or being required to work on land which they have traditionally occupied.[626]

B. Field Assessment Findings

Engagement and Remedy on Privacy Issues

Human Rights Implicated: Right to privacy; Right to freedom of expression and opinion; Right to take part in cultural life and to benefit from scientific progress; Right to take part in the conduct of public affairs; Right to information

Field Assessment Findings

- **Lack of awareness of privacy concerns among users**: Users on social media were observed sharing sensitive personal data including bank statements and checks for donations or even more sensitive information about health status without appropriate protections. Users reported being unaware of how to configure privacy settings in their social media accounts. Users also reported being unaware of how to report on content on social media.
- **Lack of policies or clear communication of policies**: Data retention policies were absent, or in some cases not clearly communicated to the customer/user even when internally present (e.g. 5 years for retention of customer data on paper).

[624] OHCHR, "OHCHR and NHRIs" (last accessed August 2015).
[625] ILO, "Forced Labour Complaint Mechanism" (last accessed August 2015).
[626] Section 6, ILO, "Update on the operation of the complaint mechanism in Myanmar, report of the ILO Liaison Officer to ILO Governing body" (319th Session, Geneva, 16-31 October 2013), GB.319/INS/INF/2.

- See Chapter 4.3 on Privacy

Engagement on Freedom of Expression and Opinion

Human Rights Implicated: Right to freedom of expression and opinion; Right to take part in cultural life and to benefit from scientific progress; Right to participate in public life

Field Assessment Findings

- See Chapter 4.1 on Freedom of Expression
- See Chapter 4.2 on Hate Speech

Engagement with Workers

Human Rights Implicated: Right to freedom of association; Right to freedom of peaceful assembly; Right to form and join trade unions and the right to strike; Right to just and favourable conditions of work; Right to freedom of expression and opinion

Field Assessment Findings

- There was a general **lack of worker-management engagement** in most companies across the ICT value chain, and only a few companies provided grievance mechanisms through which workers could raise complaints regarding their jobs and seek a resolution.
- **At fibre factories, workers were unaware of their basic association and collective bargaining rights,** for example understanding there must be a minimum of 30 members in a union**.** They did not feel the company would allow it even if it was acceptable under national law, and were concerned that joining a political party could also affect their jobs.
- **Awareness of rights to wages and benefits varied considerably**. Many workers admitted to a **very low level of understanding of their rights** vis-à-vis employers or the Government. There was also little to no information regarding labour rights or working conditions shared proactively by most companies with their workers, which will be important as a number of new labour laws, such as the *Minimum Wage Law* have recently come into force.
- See Chapter 4.6 on Labour.

Grievance Mechanisms for Workers

Human Rights Implicated: Right to freedom of association; Right to freedom of peaceful assembly; Right to form and join trade unions and the right to strike; Right to just and favourable conditions of work; Right to freedom of expression and opinion

Field Assessment Findings

- **Unskilled workers tended not to raise workplace and employment related complaints**, such as unpaid or inadequate wages, poor health and safety (H&S) standards, or barriers to unionising because they were relieved to have a job at all.
- Workers at fibre factories were able to raise complaints at meetings or anonymously through a letter box system, but **issues previously raised, such as deductions from daily wages and bonuses had failed to be addressed.**
- **Language barriers** were a commonly reported problem between managers and workers. Researchers heard that workers were often unsure whether any complaints or issues they raised were properly reported to the managers responsible.

- See Chapter 4.6 on Labour.

Engagement on Land Issues

Human Rights Implicated: Right to an adequate standard of living; Rights of minorities; Right to freedom of expression and opinion; Right to take part in cultural life and to benefit from scientific progress; Right to take part in the conduct of public affairs; Right to information

Field Assessment Findings

- There were numerous cases where individuals and communities claimed there was **no participation in informed consultation** about land acquisitions or tower or fibre projects using land in immediate proximity to their homes.
- In cases where there was prior informed consultation and participation, it was predominantly **only with the land owner/user and the (two to four) immediate neighbours** who, under the land acquisition process, were needed to sign consent forms. The wider community surrounded the tower were not believed to have been consulted. In many of those cases, **those asked to sign agreements were unclear of their purpose or content.**
- There were **very few cases** found where any ICT company or Myanmar Government had done **wider community consultation regarding the network rollout,** land needs and plans, and the ways in which the rollout would affect their lives and livelihoods, positively or negatively.
- In many cases, community members:
  - received **no prior information about the intention to acquire their land or land near their homes**, only understanding the reason was to build a tower or lay the cable line once it became apparent during construction or digging
  - were **not consulted** or given an opportunity to become informed about the **broader project of building the network**. Instead, information was given only with respect to the land registration process (see Due Process below) and compensation
  - were given **no choices** or opportunity to negotiate about the plot of land or restrictions on land use
  - often **did not know for which telecom operator** the tower construction company was building, or the cable line was being dug
  - were **not given any information to make contact or complain** either with the cable laying company, tower construction company or telecom operator
  - Commonly raised community concerns included:
  - **not knowing which company was involved** in the construction (whether fibre cable or tower).
  - **not having a company contact** in cases of issues or emergencies.
  - not being provided basic information on the safety of the tower, including:
  - whether the tower could withstand earthquakes or severe weather
  - whether they would be subjected to unsafe levels of radiation from the tower
  - whether they would be electrocuted by the tower during rain showers
  - **noise from generators powering the towers** causing a disturbance, headaches, and small cracks in walls/floors.
  - **tower sites being fenced in but not locked**, compelling villagers to "*guard*" the site to ensure children or others do not wander in.
- See Chapter 4.7 on Land

Access to Remedy for Land Grievances

Human Rights Implicated: Right to an effective remedy; Right to take part in the conduct of public affairs; Right to information

Field Assessment Findings

- As mentioned above, there were **regular reports of communities and land owners not knowing which company was responsible** for fibre cable digging or tower construction, including whom to contact in cases of emergency or grievance.
- **Cases of noise disturbance from generators powering towers were generally resolved,** in some cases by the village administrator.
- Some communities complained of **damage by the company of roads,** as well as of company-provided road repairs that failed to restore the quality of the road prior to the company's use**.**
- See Chapter 4.7 on Land

Conflict Areas

Human Rights Implicated: Right to life, liberty and security of the person; Right to just and favourable conditions of work; Right to take part in the conduct of public affairs; Right to information

Field Assessment Findings

- There were some cases in which companies attempted to negotiate access with non-state armed groups (NSAGs) to areas to lay fibre cables. **In some cases a fee was paid for this access.**
- Researchers received reports of cases of operational delays, where local groups, including armed groups, **blocked access to sites, due to lack of consultation at the site level.** While some consultation with local leaders may have been undertaken, this may not have been communicated to or accepted by all stakeholders.
- Researchers observed **fire-arms being carried by NSAGs** present during roll-out in ceasefire areas. While researchers neither observed not heard reports of shots being fired, the presence of fire-arms is a risk to the civilian population and to workers.
- Researchers also received reports from workers that they were aware that in the past landmines **may have been planted around infrastructure in conflict areas**. This led workers to avoid walking through certain areas. The measures companies took to protect their workers in such circumstances were unclear.
- See Chapter 4.10 on Conflict and Security

Myanmar Good Practice Examples:

- The Myanmar Centre for Responsible Business convened a stakeholder consultation at the request of an ICT company operating in the sector to discuss potential human rights risks for their forthcoming operations.[627]
- From 4 November to 2 December 2013, MCIT issued a call for public comments on "*Proposed Rules for Telecommunications Sector Relating to Licensing, Access and Interconnection, Spectrum, Numbering, and Competition*". Responses by 21 organisations[628] (including private sector companies, civil society organisations, and foreign governments) were posted online at www.myanmarpublicconsultation.com. This may have been the first online consultation by the Myanmar Government. Unfortunately the website is now defunct and the consultation documents and responses are no longer publicly available.
- On 21 May 2015 one of the telecoms operators held its first public sustainability seminar in Yangon, outlining human rights risks and ongoing compliance initiatives. The event was held with two-way translation.
- In March 2015, MCIT held a public forum in Yangon, focused on the health impacts on Myanmar mobile networks, with the support of the mobile industry association and one of the network providers. Research was presented focusing on international protection limits compared to radiation levels at base stations in Yangon and Mandalay. Findings showed that EMF radiation levels were far below acceptable limits set by the World Health Organisation (WHO). MCIT also produced an information brochure, including information on EMF radiation and international standards in Burmese. While the session and production of the brochure are positive steps, plans around translating the brochure into ethnic languages are unclear. This is especially important given the current geographic focus of the national telecommunications rollout. It is also unclear whose responsibility it is to distribute the brochure.
- One company has reported that their Code of Conduct covers human rights and also has a Myanmar-specific statement on human rights due diligence requirements. They have established a community outreach program with State Liaison Officers to act as a link between ethnic groups and the company, and a local hotline to which people may report grievances related to sustainability issues.[629]

[627] MCRB, "MCRB facilitates discussion between Ericsson and civil society groups" (25 July 2014).
[628] Companies that responded were Aether Company, Apollo Towers Myanmar Ltd, AVP Viom Networks, Digicel Myanmar Tower Company, Ericsson, Frontiir, GSMA, KDDI, LIRNEasia, Pan Asia Majestic Eagle Ltd, Ooredoo, Orange, Redlink, SingTel, SK Telecom, Telenor, VDB Loi, YTP. Others responding were MIDO and the US Government. See MCRB's submission: MCRB "Proposed Rules for the Telecommunications Sector" (4 December 2013).

[629] See further: Telenor, "Response by Telenor: Myanmar Foreign Investment Tracking Project", Business & Human Rights Resource Centre (last accessed September 2015).

C. Recommendations for ICT Companies on Stakeholder Engagement and Grievance Mechanisms

Stakeholder Engagement

- **Build relationships with stakeholders**: In the ICT sector, many of the stakeholders are also potential customers. Companies in the ICT value chain should have an even greater incentive to get stakeholder consultation right from the start, whether it is with communities where services are being introduced (including on-line communities) or with individuals. Since many stakeholders will not be familiar with ICTs, there is a need for basic awareness raising of ICT users on the main issues that could affect them such as data protection (see Chapter 4.3 on Privacy), protecting identity online (see Chapter 4.1 on Freedom of Expression) and appropriate behaviour (see Chapter 4.2 on Hate Speech).
- **Do not rely on Government to provide public information:** Field research indicated very little Government engagement with local communities. This means it is left to companies to inform local communities about forthcoming changes in telecommunications services, about network roll out in their area, and about forthcoming construction of this network, while keeping local government involved and informed.
- **Engage with ('offline') communities independently to build trust:** Appropriate engagement from the start matters because it: i) demonstrates respect for the community, who have experienced either neglect or reprisals until very recently; ii) is a process for providing information to and receiving information from users or communities relevant to operations; iii) enables users or communities to raise concerns and grievances; and iv) helps both companies and users or communities to understand one another's needs and expectations. There is still a high level of fear and distrust of Government and the military particularly in ethnic minority areas, given the history of human rights violations linked to the military. Companies should seek to consult communities as far as possible without the presence of military or police, and with minimal presence of local civilian authorities, so as to encourage open discussion. In some cases, trusted intermediaries may be required.
- **Engage effectively with online communities:** The growing availability of ICTs in Myanmar provides the opportunity for ICT companies (and others) to use social media, interactions through their websites, and text messaging to interact with stakeholders in a way that was not previously possible. Given the lack of online experience among the general population, companies will need to provide clear and accessible guidance, including what action is expected of stakeholders and how stakeholder views will be considered and reflected. Advertisements in official government newspapers should not be used as the sole means to publicise consultations. They are rarely read.
- **Protect the identity of those consulted where they may be at risk:** For online and offline consultation, companies will need to be concerned about the safety and security of those participating in the consultation and provide accurate information to participants about any risks of surveillance in participating in the consultations. Companies must also be particularly sensitive to undermining or exposing human rights defenders, especially land rights activists, to potential arrest and imprisonment, and respect anonymity if this is required.
- **Engage meaningfully on network rollout:** The ICT network's physical footprint is individually small, but extensive when repeated multiple times at tower sites or along hundreds of kilometres of cable trenches. It ultimately affects a significant number of individuals. It is therefore important for the network providers and their contractors

(such as tower companies and fibre cable digging companies) to have robust stakeholder engagement procedures that are grounded in a concept of respect for rights holders. This should be backed up with training to ensure that site hunters understand the core concepts of treating stakeholders fairly. With such a large number of stakeholders to deal with, and the race to construct infrastructure to meet licensing targets, there is a clear risk of stakeholders being treated only as one more item in a long checklist. While many interactions with stakeholders will be routine, the lack of awareness of many stakeholders of even what the network rollout activities are all about, much less their rights, makes many of the stakeholders, particularly in rural areas, at risk of unfair practices. This is an area where the tensions could arise between commercial pressures on tower companies and fibre laying companies to meet time targets and good practice on stakeholder engagement and even on respecting rights. While the fee companies pay for access to land for infrastructure varies according to a number of factors including assessed damages to crops, or overall disruption by workers on site, the procedures should be consistent, transparent and accessible to stakeholders and in particular those with whom companies are negotiating. See Chapter 4.7 on Land for further information.

- **Provide accurate, accessible and timely information:** Companies should be prepared to engage with stakeholders with a very low level of literacy, scientific knowledge or understanding. They should be prepared to respond in a way that is simple, accurate, balanced and understandable in local languages. This includes health and safety issues (whether the tower could withstand earthquakes or severe weather; concerns about unsafe levels of radiation from the tower (see below); concerns about being electrocuted by the tower during rain showers); information about which companies are involved in the tower site and where future questions or concerns should be directed. They should also provide clear explanations to potential customers about potential costs (such as for roaming), privacy, etc.
- **Require and monitor engagement carried out by business partners:** Sub-contractors are often the first 'face' of forthcoming operations for the rollout of the network, sales of SIM cards or sales of other ICT equipment or services. Many of these will be local companies, including very small shops. Most companies operating in Myanmar, local and foreign, are unfamiliar with the concept of stakeholder engagement, including opening their business up to receiving complaints directly from workers and local communities through grievance mechanisms. Sub-contractors, particularly in construction, will need training and incentives/ disincentives to develop positive relationships with local communities from the earliest phase of roll-out.
- **Engage constructively with civil society:** Local and international civil society organisations provide necessary support to local communities to hold government and companies to account. Companies are encouraged to engage openly with civil society and community based groups to understand their concerns and provide accurate and timely information. They should model behaviour about the right to freedom of expression that demonstrates support for the right, both in law and in practice. Dealing with criticism through constructive engagement should encourage the authorities to do the same, rather than accusing civil society groups of "*stirring up opposition*", or even arresting them [630]. When there are arrests or violence in connection with a company's operations that violate human rights, companies should raise the issue with the Government, whether quietly or publicly, individually or collectively, to express their concerns.

[630] See OHCHR, "Report of the Special Rapporteur on the situation of human rights defenders, Michel Forst" A/HRC/28/63 (29 December 2014), reporting on risks faced by land and environmental activists around some extractive projects.

- See also Chapter 4.10 on Conflict and Security concerning **stakeholder engagement in conflict areas**.

Accountability and Grievance Mechanisms

- **Provide alternative avenues to express concerns, including through operational level grievance mechanisms:** Accessing remedies in Myanmar is very difficult if not impossible in many cases. There is – with good cause – little or no faith that the judicial system can currently deliver effective remedies. The frustration over lack of access to effective remedy for real or perceived damages to livelihoods can increase tensions between communities and ICT companies and their sub-contractors. Operational level grievance mechanisms – i.e. processes that allow concerns to be raised and remedied at the operational level, rather than at far away headquarters – are therefore even more important in Myanmar, where there are: few other outlets to resolve concerns[631]. Additional Myanmar factors include unresolved legacy issues; emerging opportunities to express concerns openly; a lack of experience in local Government in addressing complaints constructively and effectively; and in some cases a lack of organisations in communities with the experience and expertise to assist in moderating and mediating between the private sector and communities. In addition, there is frequent community frustration with buck-passing between a bewildering array of contractors and sub-contractors without a core focal point for engagement and grievances.
- **Make operational level grievance mechanisms part of a broader community engagement strategy.** This should start by developing the mechanism with input from stakeholders wherever possible. Using lessons learned from the grievance process can improve ongoing engagement with communities and avoid repeating activities that have led to previous grievances. A grievance process can help companies better understand how ICT activities are being perceived and impacting, positively or negatively, on local communities, acting as an 'early warning' system.
- **Pay attention to language and literacy:** Given the variations in literacy in communities and among workers and users, there should be ways of expressing views and complaints that do not rely on reading/writing and are available to speakers of ethnic minority languages. Technical lectures to communities should be avoided.
- **Make grievance mechanisms accessible and understandable:** The field research indicated that except in a limited number of cases when some fibre companies had posted emergency contact numbers on landmarks along the cable path, communities had no information on who to turn to with concerns about telecommunications infrastructure e.g. noise, safety etc. Once the infrastructure is installed, it should include contact phone numbers on the infrastructure so that local villagers are able to contact the responsible company if they have concerns about the equipment. There should then be a process in place behind the contact numbers to ensure that the complaints are addressed. Grievance mechanisms should be implemented according to the criteria established in the UN Guiding Principles on Business and Human

[631] MCRB recently held workshops on grievance mechanisms and community engagement. See MCRB, "MCRB Holds Workshop for Business on Operational Grievance Mechanisms" (16 June 2015) and "Community Engagement by Extractive Companies is Essential for Success in Myanmar" (2 February 2015). See also the companies that have reported on their operations in Myanmar, some of which report that they have put specific operational level grievance mechanisms in place; Business and Human Rights Resource Centre, "Myanmar Foreign Investment Tracking Project", *ICT Sector* (last accessed September 2015).

Rights.[632] Good practice guidance specifically for the ICT sector is available (see section D).

- **Make online grievance mechanisms secure**: Considering the large number of potentially impacted rights holders in the ICT sector, an online grievance mechanism or reporting system accessible in the local language may be the best channel. Due to the potential vulnerability of impacted stakeholders wanting to report a violation to the company, it is important that any online grievance mechanism receives and transmits information securely. In order to build and maintain trust, companies should commit adequate resources to receiving, evaluating and responding to complaints submitted through a grievance mechanism.
- **Access to other mechanisms:** Operational-level grievance mechanisms should not impede access to other remedies, judicial or non-judicial. Additional remedy options are expected to continue to evolve in Myanmar, given the focus by the Government and donors on improving the rule of law in the country.

Table 41: Grievance Mechanisms for the ICT Sector

Existing grievance mechanisms in the ICT sector are predominantly internal corporate mechanisms, such as 'whistleblowing' systems aimed at remedying issues of labour violations, or issues arising in the supply chain, such as the use of conflict minerals. Corporate grievance mechanisms addressing violations of freedom of expression or privacy are underdeveloped, if they exist at all. Some industry initiatives, such as the Telecommunications Industry Dialogue, are reportedly still in the stages of examining options for implementing relevant grievance mechanisms.[633]

In the past decade, access to remedy for negative impacts involving ICT companies has usually been judicial rather than non-judicial. There have been court cases involving Yahoo! in China, IBM in South Africa, Cisco in China and AT&T in the USA. The Yahoo! case, which centred on the company handing over details of users who had posted pro-democracy material and were subsequently arrested and jailed, was one of the catalysts for the establishment of the Global Network Initiative (GNI).

The events of the 2011 'Arab Spring' and the 2013 revelations of mass surveillance by secret services worldwide changed the landscape of legal cases brought against ICT companies for human rights abuses, now focused more in recent years on the sale of surveillance technology and associated negative impacts on human rights. There is currently one case being considered by French courts over the sale of surveillance technology to Libya, where the company is accused of complicity in torture.[634] A verdict which goes against the company could result in the company being blacklisted or ordered to pay substantial fines.

Privacy groups have utilised other avenues to raise complaints associated with the sale or use of surveillance technology, such as the OECD National Contact Points.[635]

[632] See OHCHR, "UN Guiding Principles on Business and Human Rights" (2011), Principle 31.
[633] See Telecommunications Industry Dialogue Guiding Principles in English and Burmese
[634] FIDH, "The Amesys Case: the victims anxious to see tangible progress" (11 February 2015).
[635] See the complaints brought by Privacy International regarding the sale of surveillance technology to Bahrain: OECD Watch, "Privacy International et al. vs. Gamma International" (last accessed September 2015). See also the involvement of 6 telecommunication companies associated with the Tempora programme (where UK secret services allegedly tapped undersea fiber optic cables coming into the UK with the permission of the companies that owned them): OECD Watch, "Issue: HR violations facilitated by 6 UK telecom companies" (last accessed September 2015).

However, such complaints focus on the implementation of the OECD Multinational Guidelines and do not result in sanctions or fines against the company.

D. Relevant International Standards and Guidance on Stakeholder Engagement and Grievance Mechanisms

Relevant International Standards:

- UN Guiding Principles on Business & Human Rights (especially Principles 29-31)
- IFC: PS 1 – Assessment and Management of Environmental and Social Risks and Impacts

Guidance on Stakeholder Engagement:

- European Commission, "ICT Sector Guide on Implementing the UN Guiding Principles on Business & Human Rights"
- IFC, "Stakeholder Engagement – Good Practice Handbook for Companies Doing Business in Emerging Markets"
- Shift, "Conducting Meaningful Stakeholder Consultation in Myanmar"

Guidance on Grievance Mechanisms:

- European Commission, "ICT Sector Guide on Implementing the UN Guiding Principles on Business & Human Rights", particularly part 3.VI
- IFC, "Good Practice Note: Addressing Grievances from Project-Affected Communities"
- Access, "The Forgotten Pillar: The Telco Remedy Plan"
- European Union Agency for Fundamental Rights (FRA) "Access to Data Protection Remedies in EU Member States"
- FRA, Ongoing Project: "National Intelligence Authorities and Surveillance in the EU: Fundamental Rights Safeguards and Remedies"

4

4.10

Chapter 4.10
Security & Conflict

Dietmar Temps / Shutterstock.com

Chapter 4.10
Security & Conflict

In this Chapter:

A. Context

The race to roll out

Myanmar will probably have the fastest take-up of mobile communications in history. There is currently a race taking place to roll out the telecommunications network and secure customers among the Myanmar people, many of whom will be subscribing for the first time. Tower site hunters are continuing to actively search for sites, with an estimate of 250 towers being rolled out per month. Operators have improved coverage significantly in central and lower Myanmar, but are now beginning construction and roll out in areas such as Kachin State and Northern Shan State, with areas including Chin State and Rakhine State slated for rollout in late 2015. Operators are working to ensure that geographic targets set by the Ministry of Communication and Information Technology (MCIT) are met, including providing voice services to 75% of the country and data services for 50% of the country in 60 months[636]. This prompts companies to maximise population coverage within the confines of the geographic limits. Such dynamics may push companies to consider roll out to areas that still have active armed conflicts, as they will have dwindling options to choose 'safe' (i.e. non-conflict) areas. Other parts of the ICT value chain are increasingly operating in all parts of the country as well.

The Myanmar Government, particularly the *tatmadaw* (army), is still viewed by many ethnic minority populations with deep suspicion as a violent and predatory force. Business, especially the extractives sector, have similarly been viewed as predatory, and

[636] Myanmar Ministry of Communications and Information Technology (MCIT), "End of the Expression of Interest stage regarding the tender for two Nationwide Telecommunications Licences in the Republic of the Union of Myanmar" (21 November 2013).

there is a risk that the ICT sector could be caught up by the broader suspicions of business. Ethnic minority armed group leaders might worry that ICT will be a very well-received service, seen as being delivered or facilitated by the Government, thereby undermining their agendas and support from their communities. In other words, the telecommunications roll out may become associated with state penetration into former insurgent areas. In addition, ICTs bring 'modernisation' and the market economy which will impact on traditional cultures and livelihoods patterns. On the other hand, ICT will be seen, at least by some, as contributing to the 'peace dividend', including by providing jobs and potentially supporting ethnic languages and cultures. ICT may promote the mobility that was so long denied, for example by helping migrant workers minority groups maintain links with home. The rollout of services in ethnic areas will help ensure that a 'digital divide' is not created that could further reinforce inequality in these areas.

Armed Conflict in Myanmar

Myanmar is very ethnically diverse. However, due to complexities and nuances in terms of language, culture and self-identification, it is difficult to identify a definitive list of ethnic minorities. The current figure of 135 "*national races*" used by the Government is contested by many ethnic minority leaders who highlight its weak anthropological underpinning and believe it is an attempt to overstate the complexities for political ends. See Chapter 4.8 on Groups at Risk (specifically the sections on ethnic minorities and on the latest census).

Much of Myanmar's border areas where many of the ethnic minorities live, have been mired in non-international armed conflict for decades, and it has become a way of life for many armed groups. In the process lives, livelihoods, economies and the environment have been severely affected and sometimes destroyed (see also Chapter 4.8). Ethnic minority armed groups began fighting against the central Government shortly after independence in 1948. The *Tatmadaw* in turn launched counter-insurgency offenses. Ethnic minority armed groups operate in all seven States – Kayin, Kayah, Shan, Mon, Chin, Kachin, and Rakhine States and parts of Tanintharyi Region. Ceasefires between the Government and several armed groups began to be agreed in 1989 but were essentially only security agreements, with 'ceasefire groups' allowed to retain their arms and to control some territory. This resulted in a freeze, rather than a halt, to some of the conflicts. However fighting continued in parts of the Kayin, Kayah, and Shan States in the east of the country as armed groups there continued in their armed struggle for greater autonomy from the central Government.

In its decades-long counter-insurgency campaigns against various ethnic minority armed opposition groups, the *Tatmadaw* has committed a wide range of violations of international human rights and humanitarian law. As troops entered ethnic minority villages, they seized foodstuffs, destroyed villages, used civilians for forced labour, particularly portering, killed and tortured civilians, and forcibly displaced them. Armed ethnic minority opposition groups have also committed abuses, although to a lesser degree.[637] Ethnic grievances have centred on these abuses; the lack of self-governance and resource sharing with the central Government; discrimination and marginalisation; religious freedom; and lack of education in ethnic minority languages.

[637] For a full discussion of the human rights situation in the counter-insurgency context, see reports from Amnesty International from 1988 – 2008, and Human Rights Watch.

Conflict has greatly inhibited economic development in the ethnic border areas, and poverty rates in these areas are high. For example 73% of the population in Chin State lives below the poverty line, 44% in Rakhine State (though the World Bank's reinterpretation of the data suggests a rate of 77.9%) and 33% in Shan State; the national poverty rate is 26% (the World Bank's reinterpretation of the data reveals a 37.5% rate).[638]

Ongoing Conflicts

In June 2011 a 17-year ceasefire between major armed group, the Kachin Independence Organisation (KIO), and the Government broke down. Fighting continues in Kachin and Northern Shan States between the two groups, with some 100,000 people displaced.[639] Other armed groups there are also fighting against the *tatmadaw*, including the Ta-ang (Palaung) National Liberation Army, which is allied to the KIO. In February 2015 the Myanmar National Democratic Alliance Army, an ethnic Kokang (Han Chinese) armed group, launched an offensive against the tatmadaw in northern Shan State, where fighting is ongoing. 30,000 Kokang civilians fled to China; others were displaced internally. The President declared a state of emergency and martial law the same month, granting wide powers to the *tatmadaw* in the conflict area.[640] Since the resumption of fighting in 2011, some 200,000 people have been displaced in Kachin and northern Shan States.[641]

All of these conflicts have delayed and complicated the nationwide peace process. Moreover, both international and Myanmar NGOs have reported violations of international human rights and humanitarian law, including forced displacement and labour; torture; and arbitrary arrests by the *tatmadaw* of ethnic minority civilians in the context of the KIO/TNLA – *tatmadaw* conflict.[642]

Post-Conflict Areas and the Peace Process

From late 2011 the Thein Sein Government started a new peace initiative, engaging in talks with almost all groups and agreeing written documents. A total of 14 individual ceasefire agreements have been signed, with active talks on a nationwide ceasefire agreement ongoing between the Government and armed groups. As a result, fighting has been reduced in Kayin, Kayah, and eastern Shan States as armed groups in those areas have agreed ceasefires with the Government. On 31 March 2015 the Government and armed groups agreed on a draft text for a Nationwide Ceasefire Accord (NCA); in May armed groups met among themselves for further discussions on the draft NCA. Formal signing of the agreement has yet to take place, with both sides needing to reach a consensus inter alia on which groups are eligible to sign the document.[643] While these are historic developments, much work remains to take the next step of determining the highly political and complex questions around the Government's structure and division of power and the shape of the future armed forces. With the November 2015 elections approaching and a new Government taking power in March 2016, both the Government and armed ethnic minority groups are aware that time is running out for the National Ceasefire Agreement.

---

[638] ADB, "Interim Country Partnership Strategy: Myanmar 2012 – 2014, Poverty Analysis (Summary)" (2012).
[639] UN HCR, "2015 UNHCR country operations profile - Myanmar" (last accessed September 2015).
[640] International Crisis Group, "Crisis Alert: Deteriorating situation in Myanmar" (2 March 2015).
[641] Transnational Institute in The Nation, "Consequences of the Kokang crisis for peace, democracy in Myanmar" (29 July 2015).
[642] See for example Human Rights Watch, "Untold Miseries: Wartime Abuses and Forced Displacement in Kachin State" (March 2012).
[643] International Crisis Group, "Myanmar" (1 April 2015).

Although fighting continues in Kachin and northern Shan States, ceasefires in other ethnic minority areas are mostly holding as a post-conflict landscape emerges. Fighting has largely ceased in Kayin, Kayah, and Chin States, and the 1995 ceasefire between the New Mon State Party and the Government remains intact in Mon State. However there are legacy issues emerging, such as landmines planted by most parties to the conflicts, including non-state armed groups. The Government is not yet a state party to the Mine Ban Treaty, although in 2012 it stated an interest in acceding to it.[644] A major mine clearance operation in many parts of the border areas has yet to begin.

Ethnic minority ceasefire areas are rich in natural resources, including hydropower, hardwoods, and minerals. Ceasefires have made land more available to commercial interests, some of which are linked to the central Government and the military. Ethnic minority ceasefire groups also have business interests in their territories. At the same time these areas are highly militarised, including Myanmar troops and allied militias, ethnic minority armed groups, and armed criminal elements.

The nationwide ceasefire process will not necessarily bring an end to insecurity in Myanmar's border areas. In addition to the major armed groups at the peace table, there are numerous small splinter groups, village militias (some with hundreds of troops), and armed criminal gangs. Lack of economic opportunities, an easy availability of weapons, and weak security and rule of law mean that these areas will be characterised by insecurity for some time to come. If the peace process eventually leads to disarmament, demobilisation, rehabilitation and reintegration – which is still likely some years off – there will be the additional dynamic of former combatants with limited opportunities for lawful employment, who may resort to extortion, racketeering and other criminal activities to support themselves, as indeed some are already doing.

Intercommunal Violence

There has been a long history of inter-communal violence in Myanmar, dating back to colonial times. In 1977 and again in 1991 there were major exoduses of Rohingya Muslims [645] from northern parts of Rakhine state into Bangladesh, as a result of intercommunal clashes and abuses by state security forces. Most of the 250,000 who fled were subsequently repatriated under UN auspices, but there were no real efforts at re-integration, and the majority have no citizenship papers and were registered as "*foreign residents*" (white card holders) with fewer rights. These white cards were also withdrawn in 2015, leaving them without papers. Moreover, Rohingyas did not appear on voter lists displayed in Rakhine State during June 2015, leaving them effectively disenfranchised and unable to vote in the 2015 elections.

For over 20 years credible international organisations have reported on human rights violations against the Rohingya, including forced labour, forcible displacement, restrictions on marriage and freedom of movement, as well as the more recent violence against them.[646] Moreover successive UN Special Rapporteurs on the situation of human rights in Myanmar have expressed concerns about such violations against the Rohingya.[647]

---

[644] Landmine and Cluster Munitions Monitor, "Myanmar/Burma" (November 2014).
[645] The Myanmar Government refuses to accept the term 'Rohingya' and refers to the population as 'Bengali'.
[646] See for example Amnesty International, "Myanmar: The Rohingya Minority: Fundamental Rights Denied", Index number ASA 16/005/204 (May 2004). Human Rights Watch, "All you can do is pray: Crimes Against

A new round of deadly violence erupted across much of the state in 2012. This has mainly been anti-Muslim violence by Buddhist mobs, although in northern Rakhine State where the Muslim population is a large majority, there has also been Muslim-on-Buddhist violence. (See also Chapter 4.8 Groups at Risk). However, the most recent manifestation has been among the most intense and sustained and is partly linked to the new political realities and the competition for political power in Rakhine State. Under the military regime, the Rakhine minority was seen as a threat and systematically side-lined, and so there was effectively no political power to compete for.

Currently, there are almost 140,000 internally displaced persons in Rakhine State, many living in very poor conditions; the large majority are in Sittwe Township. Other Muslim populations have lost, or are at risk of losing, their livelihoods, compounded by longstanding restrictions on movement that prevent them travelling in search of work. Access to these populations for humanitarian organisations is a major challenge, with local Rakhine communities accusing them of pro-Muslim bias, and often intimidating humanitarian workers and blocking access to Muslim communities.

Other Security Issues

On a more general basis, to date there have been few reports of security issues around ICT infrastructure. Based on experience in other countries, once the presence of bunkers of fuels around tower base stations becomes more widely known, there could be increased incidence of theft, leading to the need for more stringent security measures or guarding of tower facilities.

B. Field Research Findings

Land
Human Rights Implicated: Right to life, liberty and security of the person; Right to take part in the conduct of public affairs; Right to information
Field Assessment Findings ▪ There were some cases in which companies attempted to negotiate access to areas to lay fibre cables with non-state armed groups (NSAGs). **In some cases a fee was paid for this access.** ▪ Researchers received reports of cases of operational delays, where local groups, including armed groups, **blocked access to sites, due to lack of consultation at the site level.** While some consultation with local leaders may have been undertaken, this may not have been communicated to or accepted by all.

Labour
Human Rights Implicated: Right to life, liberty and security of the person; Right to just and favourable conditions of work
Field Assessment Findings

Humanity and Ethnic Cleansing of Rohingya Muslims in Burma's Arakan State" (April 2013) and International Crisis Group, "The Dark Side of Transition: Violence Against Muslims in Myanmar" (Oct. 2013).

[647] Office of the High Commissioner for Human Rights, "UN rights expert calls on Myanmar to address worrying signs of backtracking in pivotal year" (18 March 2015).

- Researchers observed **fire-arms being carried by NSAGs** present during roll-out in ceasefire areas. While researchers neither observed not heard reports of shots being fired, the presence of fire-arms presents a security and safety risk.
- Researchers also received reports from workers that they were aware that in the past **landmines may have been sown around infrastructure in conflict areas**. This led workers to avoid walking through certain areas. The measures companies took to protect their workers in such circumstances were unclear.

C. Security & Conflict: Recommendations for ICT Companies

Interactions with Myanmar Military

- **Undertake enhanced due diligence regarding company interactions with the Myanmar military:** Due to the legacy of armed conflict in certain areas, and clashes still occurring in some areas, ICT companies will have to be particularly aware of the risks of human rights violations being committed by the Myanmar military near their areas of operations. Neither the field research nor other reports have indicated that the Myanmar military is providing security in connection with infrastructure rollout. However, the *tatmadaw* has played a role in security strategic assets like oil and gas pipelines in the country. The military has a long history of human rights violations in ethnic minority areas including forced labour and torture of civilians by troops, illegal taxation, and land confiscation.
- **Where military involvement is unavoidable, use international standards such as the Voluntary Principles on Security and Human Rights (the VPs**). If it is unavoidable to work have the Myanmar military provide security for network infrastructure construction or operations, operators should identify safeguards that could be put in place with them to prevent human rights abuses in connection with any of their operations. The VPs are an international initiative on security forces and human rights developed for the extractives sector but applicable more widely. They provide useful guidance for incorporating human rights into arrangements with public and private security providers (see below, Security Providers). Companies, rather than countries, can take the initiative to apply the VPs to their operations. Myanmar therefore does not need to 'join' the VPs before the standards can be adopted in-country. However since doing so requires cooperation with security forces, to be effective, the Government should understand and support the VPs and their application. Some oil and gas companies are considering advocacy to the Government to support of the VPs[648].
- **Be aware of the potential for surveillance and address consumer fears:** ICT companies that operate within those parts of the ICT value chain which may be subject to surveillance requests from the Government should understand the historical context of surveillance in Myanmar, in particular in areas of armed conflict and its often severe consequences. Currently there is a lack of appropriate legal safeguards on surveillance (see Chapter 4.4 on Surveillance). There may therefore be justifiable sensitivity among the population and civil society organisations to the possibility of continued surveillance, particularly in ethnic minority regions. There is a possibility for misunderstandings and tension if ICT companies are seen to be facilitating (and spreading) Government surveillance.

[648] See MCRB, "Myanmar Oil & Gas Sector Wide Impact Assessment" (2014), pg. 151-152.

Security Risks

- **Assess the risk of land mines**: Land mines were previously planted around Myanmar's infrastructure as (reportedly) a means of preventing sabotage by local armed groups. In addition, large swathes of the border areas are still seeded with landmines and other explosive remnants of war. There are no accurate maps of such areas seeded and in the parts of the country where conflicts are still active, new land mines are being planted. There has been no systematic de-mining in Myanmar. Ethnic armed groups generally know where land mines are in their areas of control. ICT companies will need to assess the risk of land mines being present near tower sites they are building or upgrading, as well as areas for fibre lines. Companies should avoid these areas to protect the safety of their staff and contractor staff.
- **Security risks for Muslim staff:** There exist potential security risks to Muslim staff, or staff of a company believed to be Muslim where local communities hold anti-Muslim sentiments.
- **Security risks for expatriate staff:** There exist potential security risks to expatriate ICT company staff in Rakhine State given recent protests directed at international aid workers
- **Exposure to criminal gangs:** Companies operating in conflict areas may become targets for bandit attacks, or extortion by armed groups or criminal gangs seeking to control access to areas or extort money to "*protect*" workers or facilities.

Engagement in Conflict Affected Areas

- **Consulting with non-state armed groups (NSAGs):** There are particular challenges in conducting effective consultations in conflict-affected areas. Many ethnic minority border areas have never historically come under the administrative control of the central state. Companies should build an understanding the history and dynamics of the conflict and the key stakeholders that need to be consulted, through a conflict mapping and stakeholder analysis. In areas where non-state armed groups (NSAGs) operate, it is critical to engage with them and the ethnic minority civil society groups operating in their areas. Most of these groups have bilateral ceasefire agreements with the Government that in principle authorise them to travel freely within the country (without arms) and meet with whomever they wish. They are, however, technically illegal (see Chapter 2 on the Unlawful Associations Act). It is important to recognise that some of these groups have areas of political influence and authority that are far wider than the limited territory over which they have military control. The larger NSAGs run parallel administrations, from health and education through to land registration, forestry and revenue collection. As the de facto authority in their areas, their agreement is necessary for any activities to take place. Companies should be aware of whom they are consulting with (or who those acting on their behalf are consulting with), and understand the risks of not consulting with NSAGs (but see below). It will also be important for companies engaging local contractors to understand the relationship between sub-contractors and NSAGs.
- **Consulting with communities in conflict areas:** Companies should not assume that the NSAG is representative of the views of all communities; in some cases relations may be coercive; in some cases the NSAG may be dominated by one ethnic minority and not others in the area. Companies should identify others who are representative of different constituencies, including those whose voices may not always be heard, such as women's groups or marginalised communities; as well as the main power holders (who may not always be representative). In some cases – for example, meetings with leaders of NSAGs – contacts may have to be established

through a trusted third party, who can provide a channel of communication and/or convene meetings. Experienced third party facilitators will need to be engaged to ensure that effective community consultations can take place in an atmosphere where people will be safe and confident to speak freely, something that the presence of either Government or NSAG representatives might hamper. In conflict contexts in particular, consultations with key stakeholders should be seen as a relationship-building exercise more than an information-collection exercise; if handled poorly the consultation process could put communities at risk; if handled well, the sector could provide new models for business in post-conflict areas.

- **Consultations in inter-communal conflict areas**: In areas where there are inter-communal tensions and violence, such as parts of Rakhine State, similar challenges exist. Consultations themselves could present a risk of increasing tensions or prompt violence if Rakhine communities object to consultation with Muslim communities, or object to the provision of services to other communities due to their concerns that this may give legitimacy to that community and its viewpoints. Such situations need to be handled with great delicacy, and require a detailed understanding of local dynamics; local authorities are often not neutral.
- **Understand the debate on benefits sharing:** Many of Myanmar's ethnic minority areas are resource rich with considerable economic potential, but have been exploited for the benefit of the local elite, or Naypyidaw, while the community has experienced only the negative impacts. The expectation is that discussion on this will take place as part of the post-ceasefire political dialogue. This has classically been an extractives sector issue, but given the positive benefits of access to modern telecommunications, there is a risk that ICT companies will experience similar tensions if ICTs are not rolled out to local ethnic minority populations. Universal access is thus an important objective for collective action by the sector, civil society and the Government.

Land Considerations

- **Undertake additional due diligence on land in conflict affected areas:** In conflict-affected areas, acquiring land use permits by ICT companies has added complexities. Many of these areas are not included in the national cadastre, or are considered Vacant, Fallow or Virgin lands by default. Some NSAG administrations have their own systems of land registration, including recognition of communal rights, customary rights, and shifting cultivation. Weaknesses in these systems, corruption and lack of transparency mean that local populations are not always consulted on decisions, including the granting of land use rights for private sector operations. In any due diligence, companies should consult closely with the affected communities. In some areas of contested authority, communities may not be aware that such rights have been granted, or by whom. Local armed group commanders may give authorisations without the knowledge of their headquarters.[649] The widespread planting of anti-personnel land mines in much of the border areas has restricted the use of this land by communities and other potential land users. The fact that the land has not been used by rights holders for long periods due to land mines increases the chances of dispossession of these original rights holders. Land will be particularly susceptible to land grabbing if future demining programs render it safe to use.
- **Additional land due diligence in areas of inter-communal violence:** In areas of inter-communal tension, such as Rakhine State where almost 140,000 people remain

[649] See Karen Human Rights Group, "Losing Ground: Land conflicts and collective action in eastern Myanmar" (March 2013) and TNI, "Financing dispossession" (Feb. 2012).

displaced by inter-communal violence, ICT companies will need to carry out particularly careful due diligence on the provenance of any land they seek to use. They should first establish whether there is a connection to persons displaced by inter-communal violence. Since displaced populations should be entitled to return to their homes, it is important for companies to avoid contributing to the problem, or appear to give tacit support to, or benefit from, the activities which have resulted in the displacement. Companies should obtain advice from local experts including relief agencies and CSOs operating in the area before deciding how to proceed.

Company Employed & Contracted Security Providers

- **Security Providers:** Some companies in the ICT value chain will require security guards for their towers and generators (where there are some reports of fuel and equipment theft), data centres or office buildings. It is important to ensure that contracted security providers (whether contracted directly or through a service) have had background checks to ensure security service owners, managers or guards have not been linked to past human rights abuses. They also need appropriate training on respecting human rights. Companies should ensure that working conditions and employment contracts, in line with international labour rights standards, are integral parts of the contract with the security provider, as security providers are often very poorly paid in Myanmar. Companies should consider prioritising members of local communities for security jobs, but bear in mind where this may exacerbate inter-communal tensions, depending on the choices made. As noted above, the Voluntary Principles on Security and Human Rights provide relevant guidance, despite being developed for the extractives sector. In addition, if the ICT companies find that they need active protection from private security guards, there is now an International Code of Conduct for Private Security Providers [650] that sets private security industry principles and standards based on international human rights law. The code is open to signature by companies providing security services and will soon put in place a certification system that will help to ensure company compliance with the code, providing additional assurance that service providers are trained in international human rights law principles.[651] This is a relevant reference for screening potential service providers and should serve as a goal for company commitment within a specified time period.[652]
- **Use of weapons:** Private security guards are unarmed in Myanmar, which lowers the level of risks to human rights posed by private security providers but does not eliminate all risks. Appropriate training in human rights will still be needed.[653] However in ethnic minority areas, guards may be armed, which heightens risks and requires more immediate training on the appropriate use of force and in human rights.

[650] International Code of Conduct Association, "International Code of Conduct for Private Security Providers" (2010).
[651] Ibid. See also, MCRB, "Myanmar Oil & Gas Sector Wide Impact Assessment" (2014), Chapter 4.7.
[652] See: Myanmar Times, "The rise of private security" (5 January 2015).
[653] For further guidance, see Voluntary Principles on Security and Human Rights, "Implementation Guidance Tools" (2011).

D. Relevant International Standards and Guidance on Security and Conflict

Relevant International Standards:

- The Voluntary Principles on Security and Human Rights is an initiative that includes governments, companies in the extractives sector, and NGOs. The Principles are designed to guide companies in maintaining the safety and security of their operations within an operating framework that encourages respect for human rights and which addresses working with public and private security providers.
- International Code of Conduct for Private Security Providers

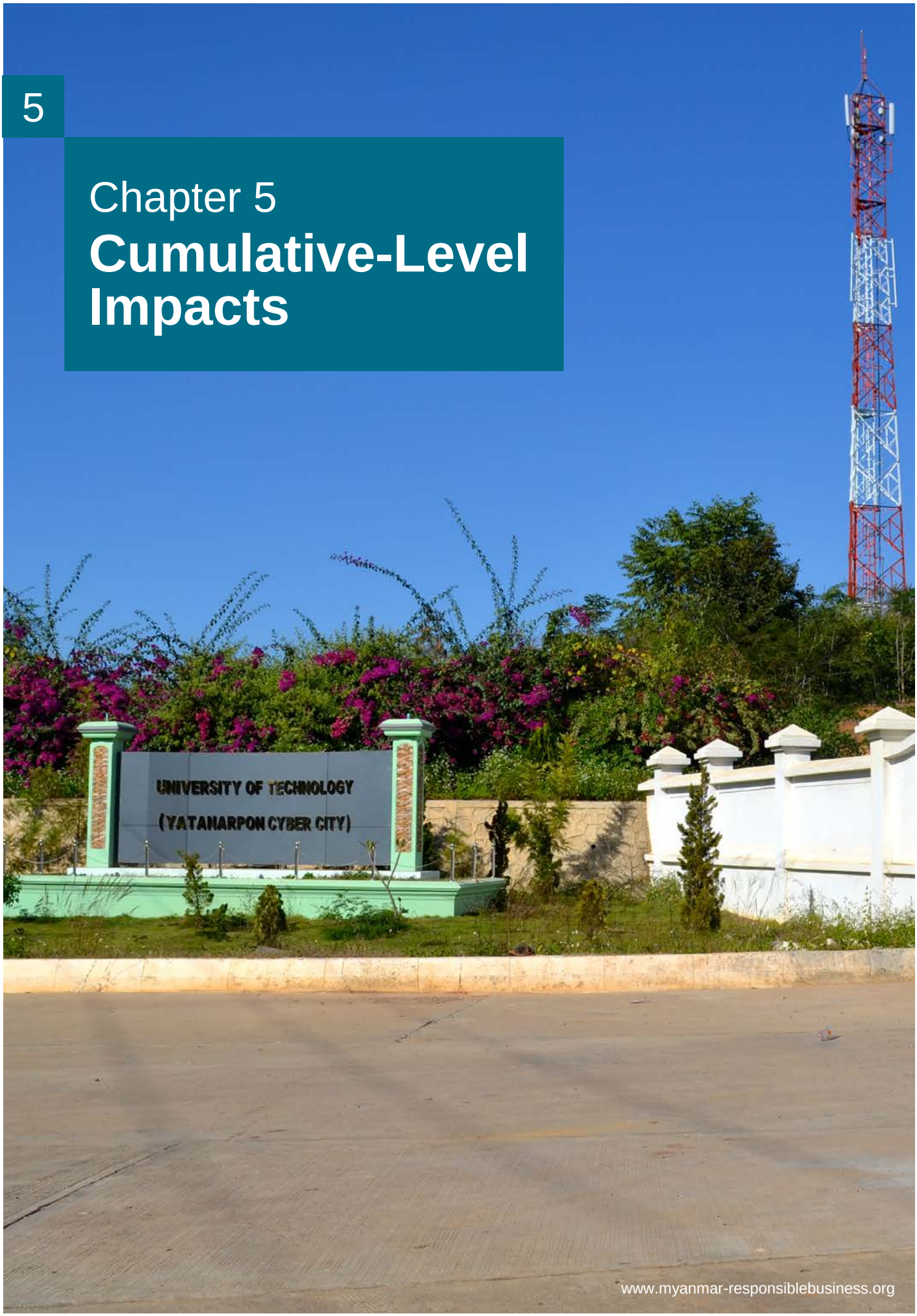
Guidance:

- The IFC/World Bank Group Environmental, Health, and Safety Guidelines for Telecommunications provide guidance on siting infrastructure and other aspects of community safety.[654]
- The World Bank-supported Myanmar Telecommunications Sector Reform Project Land Lease Guidelines provides valuable guidance for other ICT companies involved in land acquisition, including calling for the identification of the presence of ethnic minorities during scoping and screening phases.[655]

[654] IFC, "Environmental, Health, and Safety Guidelines for Telecommunications" (April 2007).
[655] World Bank, "Myanmar - Telecommunications Sector Reform Project: environmental and social management framework (Vol. 2): Land lease guidelines" (English) (2013).

5

Chapter 5
Cumulative-Level Impacts



5

Chapter 5
Cumulative-Level Impacts

In this Chapter:

A. Introduction

This Chapter looks briefly at successive, incremental and combined environmental and social (including human rights) impacts from multiple projects or multiple ICT activities located in the same region or affecting the same resource.[656] Consideration of cumulative impacts is of growing importance in regions where environmental and social systems have reached their maximum capacity to absorb and adapt to additional impacts (as may be the case in parts of neighbouring China),[657] but they can also be equally as important to consider in regions that will undergo significant growth, as is the case in Myanmar.

The study of cumulative impacts is often associated with projects with a large physical footprint – extractives and infrastructure – rather than industrial sectors with a small footprint like ICT. The majority of the ICT value chain is service-based. Its cumulative impacts are mostly social and occur at the sectoral and societal level (see further Chapter 3). Nonetheless, the sector may still create cumulative impacts on the ground particularly given its projected growth trajectory in the country. These should be considered and addressed in future Government and company planning. Examples could include repeated digging of ducts for cabling, rather than the laying of a single duct for multiple users, or the erection of multiple towers in one location rather than shared facilities. Initial attempts by Government to encourage sharing of infrastructure (towers and power generation) were not successful due to the speed of the rollout and differences in business models between operators. However, the Government did take the initiative to bring the two operators together to discuss their site plans and encourage communication between tower companies to try to limit the number of duplicate tower sites in the rollout.

Infrastructure used in the ICT sector (buildings or network infrastructure) placed in proximity adds incremental impacts to other existing, planned, or reasonably predictable future projects and developments, leading to an accumulation of impacts. Environmental and social impacts from one project alone are not always significant. It is the building up of smaller impacts over time, or within the same physical footprint, that have a cumulative

[656] Based on the definition in Franks, Brereton and Moran, "Cumulative Social Impacts," in Vanclay and Esteves (Eds), *New Directions in Social Impact Assessment: Conceptual and Methodological Advances*, (2011). They are sometimes also referred to as "collective impacts."
[657] Ibid, pg. 202

effect. Sometimes a series of smaller events can trigger a much bigger environmental or social response if a tipping point is reached, changing the situation abruptly (e.g. where there is a rapid influx of people seeking jobs at, or in the vicinity of, newly established projects, the 'boomtown effect'). They can also be triggered by poorly designed policies that prompt companies to make the same mistakes over and over again.

The resilience of the environment or society to cumulative impacts depends upon both the nature of the impacts and the vulnerability (or sensitivity) of the society or ecosystem (i.e., the degree to which they are susceptible to and unable to cope with injury, damage, or harm).[658] Cumulative impacts can be negative (e.g. outmigration due to cumulative land acquisition results in Government withdrawal of health services) or positive (e.g. cumulative economic developments in the area justifies opening of a public health clinic). In some cases, cumulative impacts can have both positive and negative effects.

If not managed, cumulative impacts can overwhelm environmental or social 'carrying capacity' to withstand or recover from the changes and result in human rights impacts. They can act upon:

- **Institutions** – the accumulated impacts overwhelm the local capacity to provide services, including protection or fulfillment of the population's human rights, such as education or health, providing remedies, or managing/changing the course of events
- **Society** – the rapid onset and acceleration of the changes overwhelms societal structures and capacity to manage change, which may eventually lead to a rise in tensions or violence and a potential breakdown in law and order
- **Environment** – the biophysical impact surpasses the environment's carrying capacity, with negative impacts on the right to water or other livelihood or health impacts.

B. National Context

As a first step in recognising that ministries and regional authorities need to consider cumulative impacts in the context of Myanmar's rapid development, the Framework for Economic and Social Reforms (which sets the medium-term strategy for Myanmar's development) identifies cumulative impacts as an important consideration:

> *"Planners and policy-makers will need to consider the longer-term dimensions of a balanced strategy of economic, social, environmental and cultural development, recognising particularly that stakeholder groups can be affected simultaneously by projects or programs that are considered independently of each other without acknowledging their cumulative impact on particular stakeholders. Decision-making and monitoring processes will need to be open to such cumulative impacts. Taking a longer-term perspective may also help to resolve apparent trade-offs in situations where greater emphasis on equitable development in the short-term contributes to greater sustainability and economic growth over the longer term."*[659]

[658] IFC, "Good Practice Handbook on Good Practice Handbook, Cumulative Impact Assessment and Management: Guidance for the Private Sector in Emerging Markets" (2013).
[659] Government of Myanmar, "Framework for Economic and Social Reform - Policy Priorities for 2012-2015 towards the Long-Term Goals of the National Comprehensive Development Plan (FESR)" (January 2013), para 92. In addition, the current draft of the E(S)IA Procedure includes references to cumulative impacts, especially for complex projects

Myanmar has an ICT Master Strategy, but this strategy does not consider the regional implications of the strategy and therefore does not lay the groundwork for considering cumulative impacts of ICT developments in any particular areas. The regulatory framework for Environmental Impact Assessment (EIA) requires consideration of cumulative impacts although practice is as yet undeveloped. However, most ICT projects are unlikely to require an EIA in Myanmar unless facilities or infrastructure are located on land of special importance, such as cultural sites or national parks. Myanmar does not appear to have yet considered the steps it will need to take to deal with e-waste.

C. Research Findings

The ICT Master Plan identifies several developments that could lead to cumulative impacts.

ICT Parks

The ICT Master Plan sets out the intention to set up additional ICT Parks, building on the models of the Myanmar ICT Park in Yangon (established in 2001) and Yatanarpon Cyber City in Pyin Oo Lwin (established in 2007) which is currently underutilised. In 2015, the Myanmar Computer Federation announced that a new 300-acre ICT Park is to be constructed outside of Yangon in Thanlyin, noting that significant foreign investment will be needed to complete construction.[660] Thanlyin is adjacent to Thilawa Special Economic Zone, south-east of Yangon. The Follow-up Report also suggests encouraging the development of such parks in other Myanmar's Special Economic Zones[661]. The *SEZ Law* also provides for land acquisition and compensation to land users.[662]

As noted in the ICT Master Plan Follow Up Report,[663] there are benefits for firms based in the ICT Parks. Colocation facilitates collaboration to resolve problems, initiate technology forums and seminars, and promotes networking. [664] For such parks to be successful, the Follow Up Report suggests initial incentive policies such as providing discounts on land price, and abatement of lease rates, national and local taxes.

However concentrations of businesses in one area also create greater potential for negative cumulative environmental and social impacts, including the longer term impact of industrial activities within the area, transport infrastructure in and out of the zone, and demands on public services such as housing, healthcare and education for the workers and their families. In some countries, SEZ Laws reduce the labour protections for workers within the zones as further inducement to business. The Myanmar *SEZ Law* does not waive Myanmar labour requirements; however few Myanmar labour laws are in line with international labour standards (See Chapter 4.6 on Labour). Moreover, there are concerns with the land acquisition and resettlement processes the various SEZs that could be repeated by large footprint ICT Parks.

Outsourcing

The Follow Up Report to the ICT Master Strategy notes that "*Myanmar's ICT industry has strength in the software industry and being supplier of overseas companies' ICT*

[660] Eleven Myanmar, "Thanlyin Picked for ICT Park" (2015)
[661] Dawei, in the southeast of the country; and Kyaukphyu, in Rakhine State.
[662] See: MCRB, "Land Briefing" (March 2015), pg. 15.
[663] MCIT, KOICA, ETRI, "The Follow-up Project of the Establishment of ICT Master Plan in Myanmar" (2011).
[664] Ibid, pg. 165.

outsourcing demand by subcontract or dispatch". It encourages ramping up Government demand as a way of stimulating both demand for such services and the supply of software engineers as well as deregulation to stimulate demand.[665]

Table 42: India Case Example on Business Process Outsourcing

After independence in 1947, India began to invest in institutes of higher education that provided high-quality science and technology training, producing tens of thousands of scientists and engineers. When India liberalised its economy in 1991 and started courting foreign investment, among the first companies to capitalise on the opening were information technology companies, which set up back offices, business process outsourcing (BPO) centres, and software development centres. Today, some 2.8 million people work in the BPO sector, and annual revenues exceed US$11 billion.

The ICT sector has created well-paid jobs for India's skilled workforce and more critically, for Indian women. The labour force participation rate of women in India has traditionally been low – only about a third of Indian women are part of the organised labour force.[666] There are many reasons for this, including early school dropout rate, particularly in rural India,[667] pressure on getting young girls and women married early[668] and early child-birth. Women represent some 40% of the workforce[669] in the BPO sector, and their increased earning power has enhanced their social standing and shifted the power balance between the sexes.

However, many of these companies operate in export processing zones, where certain trade union rights are suspended[670]. That also means that some of the benefits employees can expect are not available, including, for example, health and maternity benefits in line with Indian laws. Moreover, many companies keep hours to align schedules with office hours in the West, which means some workers work on all-night shifts – which can have an adverse impact on family life and their economic, social and cultural rights.[671] Women who work night shifts or late hours have occasionally been assaulted sexually on their way home.[672]

The ICT sector has created job opportunities outside major metropolitan areas. Towns that want to attract BPOs have invested in creating infrastructure, including access to water and power for the industry, which has improved living standards in areas that previously did not have such infrastructure. Cumulatively, there are significant benefits for those who work at the centres and those who live in those towns, affecting many rights, including the right to an adequate standard of living,

[665] Ibid, pg. 152.
[666] ILO, "India: Why is women's labour force participation dropping?" (13 February 2013).
[667] Internetional Journal of Current Research, "Reasons for rising school dropout rates of rural girls in India - An analysis using soft computing approach" (24 May 2011).
[668] "Early Marriage In South Asia: A Discussion Paper" (date unknown).
[669] Dr. Kousar Jahan Ara Begum "Women & BPOs In India" *International Journal of Humanities and Social Science Invention* (May 2013).
[670] Amandeep Sandhu, "Why Unions Fail in Organising India's BPO-ITES Industry" *Economic and Political Weekly* (14-20 October 2006).
[671] Dr. Sunitha V Ganiger "Women in BPO's and its Impact on Family: A Sociological Analysis" *Indian Journal of Research* (February 2014).
[672] India has harsh punishment for sexual violence, including the death penalty. See for example: The Indian Express, "SC confirms death for Pune duo in rape, murder of BPO employee" (10 May 2015).

and other rights associated with structured, formal employment, such as health benefits from companies that adhere to relevant laws.

The Report highlights the many benefits to the Myanmar economy including stimulating better education of software engineers, improving competitiveness, bringing the benefits of ICT to other sectors in the Myanmar economy. These many benefits should be weighed together with relevant regional experiences of the social impacts of developing a large sector of outsourcing services and considered as an integral part of the planning for such an expansion. While the job opportunities would provide an important step up the ladder, those developments should go hand in hand with ensuring decent work. The ILO is developing a Decent Work programme in Myanmar[673].

Manufacturing

Currently, there is a limited ICT manufacturing in Myanmar, and the hardware industry is mainly based on trading and assembling. Limited manufacturing of fiber cable takes place at Yatanarpon Cyber City.[674] The follow up to the ICT Master Plan suggests Government financial and administrative support to encourage ICT manufacturing, noting that "*lately Myanmar is becoming more attractive location as it has competitive salary level comparing to other countries*"[675]. It makes a case for developing a handset industry.

Moving up the value chain in manufacturing could provide significant benefits to the Myanmar economy. But Government planners should also consider the environmental, social and human rights impacts of developing manufacturing clusters in the ICT sector, considerations that are currently absent from the ICT Master Plan and the Follow-up Report.[676] There are clearly economic benefits of developing manufacturing hubs. These need to be addressed together with the costs to the local environment, community and workers. There is increasing attention on the impact on human rights of the electronic sector in the global economy. This has prompted the creation of several multistakeholder and industry-led initiatives to address the rising legal and reputational challenges to the sector.[677]

D. Guidance on Cumulative Impacts

- IFC, "Good Practice Handbook on Cumulative Impact Assessment and Management: Guidance for the Private Sector in Emerging Markets"
- UNGC "Business & Human Rights Dilemmas Forum: Cumulative Impacts"

[673] ILO, "National Triparite Dialogue: Presentation on Decent Work Country Program (Myanmar)" (Dec 2015).
[674] Zaw Min Htwe, "Oppurtunities and Challenges for a Foreign Invested Company at Yatanarpon Cyber City, Myanmar" (December 2011), p. 17
[675] MCIT, KOICA, ETRI, "The Follow-up Project of the Establishment of ICT Master Plan in Myanmar" (2011), pg. 169.
[676] See for example GoodElectronics.
[677] See for example the Electronics Industry Citizenship Coalition and Global E-sustainability initiative.

Annex A: Additional Information on SWIA Methodology

A. SWIA Phases

The SWIA process follows well-established impact assessment steps. For each step of the process specific tools or approaches have been developed, which are described below.[678]

Table 43: SWIA Phases

I. Screening	
Objective: Select economic sectors for a SWIA based on several criteria: ▪ the importance of the sector to the Myanmar economy ▪ the complexity and scale of human rights risks involved in the sector ▪ the diversity of potential impacts looking across the sectors ▪ human development potential ▪ geographical area **Tasks:** ▪ Informal consultations were held inside and outside Myanmar to develop and verify the selection of sectors.	**Key Outputs / Tools** ▪ Selection of 4 sectors for SWIA: Oil & Gas (published Sept. 2014), Tourism (published Feb. 2015), ICT (published Sept. 2015) and Agriculture (subsequently changed to Mining – forthcoming)
II. Scoping the ICT sector in Myanmar	
Objective: Develop foundational knowledge base to target field research for validation and deepening of data collection. **Tasks:** • Commission expert background papers on: the ICT sector; the legal framework; land and labour issues • Stakeholder mapping	**Key Outputs / Tools** • Scoping papers • SWIA work plan
III. Identification and Assessment of Impacts	
Objective: Validate foundational knowledge base with primary data collected through field research from targeted locations across Myanmar. **Tasks:** ■ Four rounds of field team visits to three different locations	**Key Outputs / Tools** ■ Questionnaires ■ Internal fact sheets on various business and

[678] This table has been gratefully adapted from the presentation used in Kuoni's HRIA of the tourism sector in Kenya.

each time collecting qualitative data from:

- Communities potentially affected by ICT operations, covering issues including: ICT use; Livelihoods; Consultation; Land use; Environment; Labour; Migration; Children; Gender; Security; Indigenous Peoples/Ethnic Peoples.
- Managers of ICT companies, covering issues including: Customer/user privacy and security (including lawful interception and surveillance); Freedom of expression (including censorship and hate speech); Working Conditions; Community impacts (including land use).
- Employees and workers of ICT companies, covering issues including: Working conditions; Health and safety of workers.
- External stakeholders, covering issues including: The impacts of ICT operations for local or national authorities, NGOs and CSOs, international organisations, journalists, political parties, schools and monasteries.

- Compile and synthesise field data, including IHRB/DIHR trips to debrief with research teams in Yangon
- Further desk research

IV. Mitigation and Impact Management

Objective: Identify measures that will help avoid, minimise, and mitigate potential impacts of the sector.

Tasks:

- Synthesise information on potential impacts at the three levels: sector, cumulative and project in order to identify considerations for companies and Government to prevent or mitigate potential impacts

Key Outputs / Tools

- Initial synthesis reports of field findings

V. Consultation & Finalisation of the SWIA Report

Objective: Present SWIA findings and conclusions, as well as recommendations to be validated through consultations with representatives of Myanmar Government, ICT companies operating/planning to operate in Myanmar, and representatives of civil society organisations, some of whom represent those affected by ICT operations in Myanmar, trade unions, international organisations, donor governments.

Tasks:

- Iterative drafting of main SWIA chapters
- Translations for consultations
- Consultations in Yangon, Naypyitaw and Europe
- Revisions to draft SWIA
- Finalisation, publication and dissemination of the ICT SWIA

Key Outputs / Tools

- Draft SWIA report in English and Burmese
- Slide pack summarising the SWIA findings for consultation
- Consultation report
- Final ICT SWIA report and dissemination

human rights issues in Myanmar
- Ethical research policy
- Field safety guidelines
- Interview summaries
- Reports of stakeholders consulted

B. What is Different about a SWIA compared to a Project Level Impact Assessment

- **Wider audience:** A project-level environmental, social or other impact assessment is typically carried out by or for an ICT company to fulfill a regulatory requirement as a

step in gaining permission to operate. SWIA are intended for a much wider audience: Government and Parliamentarians, business, local communities, civil society, and workers and trade unions.

- **Aims to shape policy, law and projects:** SWIA look at the national context, national frameworks, legal contracts (where available) and business practices, and identifies what actions will help shape or impede better human rights outcomes for the sector. The findings inform the analysis and recommendations at the core of the SWIA for a range of audiences.
- **Information goes into the public domain**: Company-led human rights impact assessments (HRIA) are typically confidential, and environmental or social impact assessments may be also unless disclosure is required. The whole rationale behind the SWIA is to make the document a public good for the purpose of informing and thereby improving practices and outcome of business investment.
- **Looks at 3 Levels of Analysis**: The SWIA looks at the impacts of the sector and to do this uses three levels of analysis: sector, operational and cumulative levels.
- **Does not replace the need for an individual human rights and/or environmental and social impact assessment by a company:** The SWIA does not replace the need for an operational-level impact assessment where required or desirable. Instead the SWIA helps *inform* a company's assessment, as it gives an indication of the kinds of human rights impacts that have arisen in the past in the sector. This helps to forecast what future impacts may be. A SWIA may be particularly relevant at the scoping stage of a company's operations. The SWIA also alerts to potential legacy issues that incoming operations may face. Such assessments will have to examine the specific situation of the forthcoming project within the particular local context and in doing so, may also uncover new potential impacts that were not picked up in the SWIA. It is therefore not a checklist, but a guide for considerations in subsequent impact assessments.
- **Does not replace the need for conflict risk assessments:** Given the history of conflict in certain areas of the country, companies operating in those areas might want to carry out specific conflict risk assessments covering the areas in which they plan to operate. The limited number of people interviewed and places visited within the framework of this SWIA is not sufficient to develop a comprehensive analysis of drivers of conflict. However, such a limitation is inevitable in the rationale for the SWIA, which cannot expect to get this level of detail across the country. Furthermore, the types of interviewees would need to be expanded in order to more effectively capture conflict impacts, including conflict experts, ethnic armed group and community leaders.
- **Takes a broad view of what a human rights impact includes.** As HRIA methodology evolves, there has been an accompanying discussion about what distinguishes a human rights impact from other types of social impacts in particular. The SWIA takes a broad view of what constitutes a human rights impact, as there are a wide variety of actions that can ultimately result in human rights impacts and because it is intended to support an approach to responsible business conduct in the country which will require addressing all these issues.
- **Takes a practical view on distinguishing different types of impact assessments.** In certain industry sectors (such as extractives), environmental and social impact assessments (ESIA) are often a routine requirement. This has led to global discussion about what distinguishes an SIA from an HRIA, potentially diverting attention from getting on with the process of assessing and addressing potential impacts. The approach taken in this SWIA is that the labels that are given to the process are less important than getting the process and the content covered in a manner that is compatible with human rights – much depends on the quality of the ESIA/SIA. A good

quality ESIA/SIA comes close to addressing many human rights issues but may not pay sufficient attention to civil and political rights, and in considering risks to human rights defenders, which can be relevant to extractive projects.[679] See Table 44 below.

- **Does not establish a baseline but instead describes the situation for the sector at a moment in time.** The SWIA does not purport to set out a baseline of conditions at the project level; this is a task for operator's project-level ESIA. Chapter 3 on Sector Level Impacts, and the national context discussions at the beginning of each of the ten parts of Chapter 4 on Operational-Level Impacts and at the beginning of Chapter 5 on Cumulative-Level impacts, sets out the current context around the enjoyment of human rights at the national level, and gives some indication regarding future trends as well as particular areas that are high-risk based on past in-country experiences.
- **Would provide relevant information for a sector master plan or strategic impact assessment.** While these have not been used to date in Myanmar, the Government is in the process of revising at least three ICT related Master Plans.

Table 44: Six Key Criteria for Assessing Human Rights Impacts

In order to adequately assess human rights impacts, the impact assessment process and content should reflect the six criteria listed below[680]

Standards
The impact assessment needs to be based on international human rights standards. Human rights constitute a set of standards and principles that have been developed by the international community. This establishes an objective benchmark for impact identification, severity assessment, mitigation and remedy.

Scope
The scope of an assessment should include actual and potential human rights impacts caused or contributed to by a company, including cumulative impacts, as well as impacts directly linked to a project through business relationships such as with contractors, suppliers, JV partners, and government and non-government entities.

Process and engagement
The impact assessment, including associated engagement and consultation activities, should apply the human rights principles of participation, non-discrimination, empowerment, transparency and accountability. This promotes attention to process, not just outcome, and can help to create "buy-in" in the impact assessment among relevant stakeholders. Inclusive engagement throughout the impact assessment process is a key component, in a manner that is gender sensitive and takes into account the needs of vulnerable individuals and groups, providing capacity building or assistance where needed to promote their meaningful participation.

Assessing and addressing impacts
Impacts should be assessed according to the severity of their human rights consequences. This means including the assessment criteria of scope, scale and ability to remedy the impact, and taking into account the views of rights-holders

[679] See: OHCHR, "Report of the Special Rapporteur on the situation of human rights defenders, Margaret Sekaggya", A/HRC/19/55 (2011), sections III & IV.
[680] Developed by the Danish Institute for Human Rights.

and/or their legitimate representatives in determining impact severity. Addressing identified impacts should follow the standard mitigation hierarchy of "avoid-reduce-mitigate-remedy". Where it is necessary to prioritise actions to address impacts, severity of human rights consequences should be the core criterion.

Accountability and transparency
The impact assessment should consider the differentiated but complementary duties and responsibilities of government and non-government responsible parties for addressing identified impacts. For company responsibilities, this would include assigning to relevant staff members actions to avoid, mitigate and remedy impacts. The impact assessment and its associated communications should be transparent and provide for effective ways for rights-holders to hold the responsible parties to account for how impacts are identified, prevented, mitigated and/or remedied.

Interrelated impacts
Identification and management of impacts should take into account the interrelatedness of various environmental, social and human rights impacts. For example, depleting a community water supply will have an impact on the right to water, but may also have interrelated impacts on the right to education of children who may need to walk longer distances to collect water and are therefore less able to attend school.

C. Limitations of the ICT SWIA

- **Non-attribution:** The team made a decision not to attribute practices, good or bad, to particular places, companies, or individuals and therefore have not listed specific stakeholders engaged during the research. The SWIA uses existing experiences to identify opportunities to improve new and existing projects in the sector.
- **Thirteen locations in six States/Regions visited:** The ICT SWIA field research focused on six States/Regions where ICT operations are underway and that are representative of a range of ICT contexts in Myanmar: urban and rural ICT usage; tower rollout in urban, rural and conflict affected areas; ICT parks and facilities; internet cafes and phone and SIM shops in urban and rural settings; amongst others. While this does not include all areas where current or future ICT operations are taking place, the SWIA's Recommendations are representative enough to be generally applicable to existing and future ICT operations in Myanmar that are not in conflict. The findings highlight trends seen across the six research locations and are therefore not meant to provide detailed analysis of particular types of projects or regions.
- **"Online" and "Offline" focus:** This SWIA for the ICT sector looks at both "online" human rights risks (such as impacts to freedom of expression and privacy from ICT use) and "offline" human rights risks (such as labour rights impacts from tower or fiber line construction, or livelihoods impacts of communities). The ICT SWIA does not consider ICT manufacturing and production impacts in detail as such activities were fairly limited in Myanmar at the time of preparation of the Report (i.e. 2014/15).
- **Existing, not planned, operations:** It was specifically decided to do the field research in locations with existing ICT operations, rather than prospective areas for rollout or other ICT activities. Given the tensions that have surrounded some industrial projects to date in Myanmar, there was a concern that asking about potential projects in certain areas (without knowing whether projects would actually materialise) might create concerns in communities and potentially build expectations (good or bad) that were not fulfilled. In addition, given the inexperience of many Myanmar communities

with being able to express their concerns publicly, the relative lack of experience with ICT or other technical operations in the country to date, the project team decided that research with communities that had experience with nearby ICT projects would be able to provide more relevant data for the research. In addition, as Government permission was needed to carry out the research and given sensitivities surrounding the other sectors, it was considered more likely that Government permission would be granted to review existing rather than prospective projects.

- **Rapidly changing dynamics:** A challenge of conducting a SWIA in Myanmar is that the country continues to undergo rapid social, economic, political and regulatory change. As a result, past experiences, both positive and negative, may not always be relevant to future operations. Examples of good practice from the previous era where companies would rightly try to insulate themselves from interaction with the Government are far less likely to be appropriate in a new era of openness. Prompting the Government to support responsible business approaches may be a more appropriate approach.
- **Conflict expertise:** The interviewers were experienced social science researchers but did not have sufficient experience or training in questions of diversity and exclusion to sufficiently explore ethnic grievances and the dynamics of conflict (both armed conflict and inter-communal violence). Given Myanmar's recent history, addressing this would require very careful selection and intensive training of interviewers, and even then there would likely be remaining limitations with gathering all required information through qualitative information.
- **Limitations due to lack of permission:** In some instances no permission was granted to speak to workers of ICT companies or to community members, or permission was delayed, which resulted in limited time in order to conduct interviews. However generally both the authorities and most companies have been collaborative and open to granting access to the SWIA field teams and to sharing information.
- **Access limitations:** While the SWIA field teams tried to conduct workers' interviews outside of their workplaces and without the presence of management, this was not always possible. This may have led to different interview responses than if interviews were confidential.

D. Field Research Methodology & Interviews

Field Research Methodology

The ICT SWIA is comprised of both primary and secondary research. For the primary research, teams of two researchers (plus a local facilitator, translator and driver as needed) visited thirteen different locations over four different field trips (see location map below).

The field teams used qualitative research methods that were adapted to the local contexts to take account of the sensitivities of localised issues (such as potential conflict or tensions) while being sufficiently standardised to allow for coverage of all major human rights issues and comparison of findings.

The field researches used a set of assessment questionnaires to structure their meetings and guide their conversations (rather than as checklists). The questionnaires are based on DIHR's Human Rights Compliance Assessment Tool (HRCA),[681] a tool to enable companies to identify and assess human rights compliance in their operations (a more generalised copy of the interview questionnaires will be on the MCRB website).[682]

The questionnaires covered four overarching stakeholder groups and interviews were held one-to-one, in small groups and through focus group discussions:

- Managers of ICT companies and sub-contractors
- Workers of ICT companies and sub-contractor
- Communities
- Other external stakeholders (local or national authorities, NGOs, international organisations, journalists, political parties, schools and monasteries)

Open questions were used as much as possible, in order to allow respondents to answer using their own thoughts and words, and raise the issues they considered as important. All interviews were documented with written notes and in most cased voice recorded with permission of the interviewees. Most interviews were conducted in Burmese, while local intermediaries translated in meetings with local community representatives where regional languages were used. The issues in Table 45 below were covered in the field research questionnaires.

Table 45: Topics Covered in SWIA Questionnaires

Communities who are potentially affected by ICT operations, covering ICT issue areas including: ICT uses, livelihood, consultation, land use, environment, labour, migration, children, gender, security, indigenous peoples/ ethnic peoples.	**Managers** of ICT companies and their contractors and suppliers, covering issues such as: customer/user privacy and security (including lawful interception and surveillance), freedom of expression (including censorship and hate speech), working conditions, and community impacts (including land use).

[681] DIHR, "Human Rights Compliance Assessment" (accessed 15 July 2014).
[682] http://www.myanmar-responsiblebusiness.org/

Employees and workers of ICT companies and suppliers' employees, which covers issues related to working conditions and health and safety of workers.	**External stakeholders** with questions related to the impacts of ICT operations for local or national authorities, NGOs, international organisations, journalists, political parties, schools and monasteries.

ICT Field Visit Locations

The SWIA field research was carried out in the following locations:

Figure 6: ICT SWIA Field Research Locations

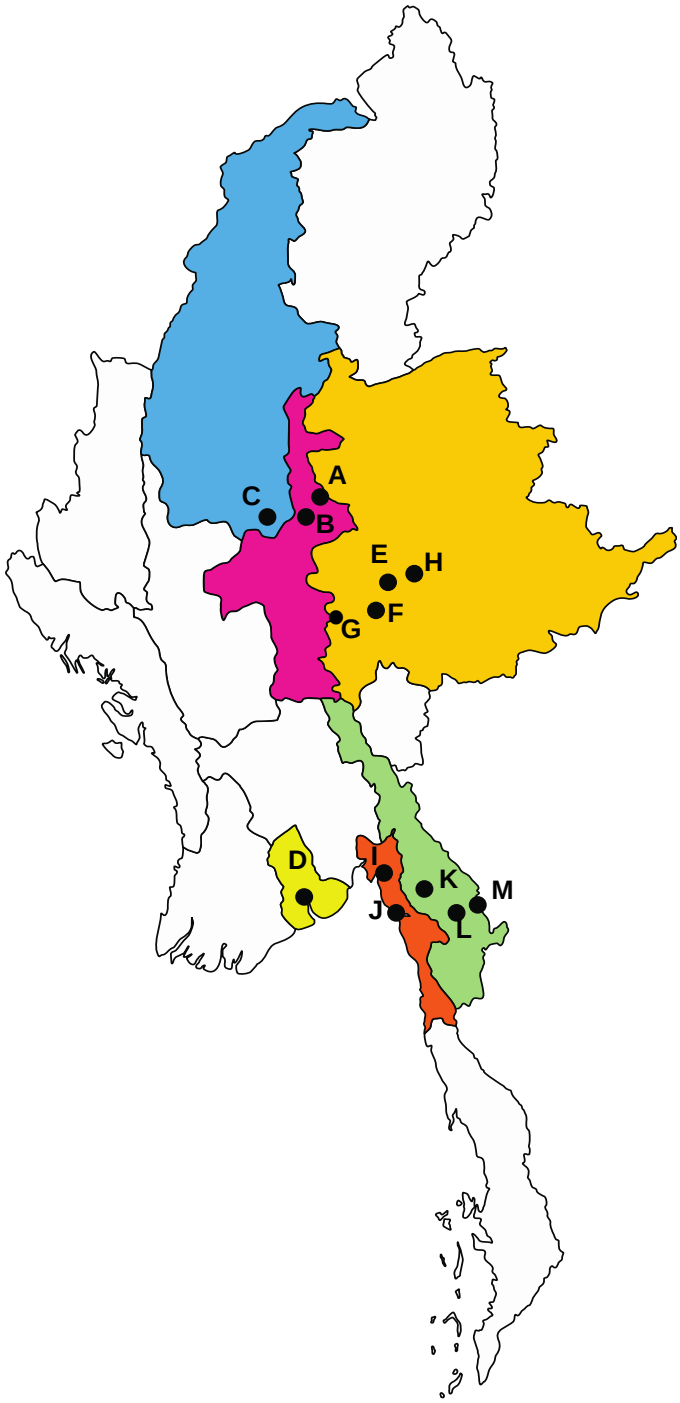
1st round of field visits: Nov-Dec 2014
Mandalay Region:
A. Pyin Oo Lwin
B. Mandalay
Sagaing Region:
C. Sagaing

2nd round of field visits: Dec-Jan 2015
Yangon Region:
D. Yangon

3rd round of field visits: Jan 2015
Shan State:
E. Taunggyi
F. Nyaungshwe
G. Shwe Nyaung
H. Hopong

4th round of field visits: Feb 2015
Mon State:
I. Thaton
J. Mawlamyine

Kayin State:
K. Hpa-An
L. Kawkareik
M. Myawaddy



Overview of Stakeholders Consulted

Researchers often began visits to different towns by speaking with the local township or village authorities. This helped provide an initial understanding of some of the main issues affecting or concerning the community as a whole. Researchers then conducted individual interviews and focus group discussions to discuss in more detail but without the authorities present in order to gain insights from other perspectives. The interviews generally covered the issues in the questionnaires.

Table 46 below presents a breakdown of the discussions with 181 individuals from different stakeholder groups – 143 within individual interviews and 38 attending focus group discussions. Numerous individual meetings were held in Yangon with ICT company representatives (both Myanmar and international) to present SWIA project plans and discuss their operations, policies, due diligence processes and grievance systems. Additional meetings were also held in Naypyitaw and Yangon with Government Ministers and officials.

In addition, meetings were held with various ICT industry associations, donor organisation representatives, civil society groups and governments outside of Myanmar to explain the SWIA methodology and provide the opportunity to give input on the research.

Table 46: ICT SWIA Stakeholder Interviews Conducted

Type of Stakeholder and Numbers of Male /Female Interviewees	Field Assessment Locations
Armed Groups 2 Individual interviews 1 Focus group discussion (FGD) 6 Male	**Thaton, Mawlamyine, Hpa-An, Myawaddy** **Mawlamyine (1 FGD**: 1 ethnic armed group) **Myawaddy (1 Individual**: 1 ethnic armed group) **Hpa-An (1 Individual**: 1 ethnic armed group)
Business 42 Individual interviews 2 Focus group discussions (FGD) 49 Male 4 Female	**Pyin Oo Lwin, Sagaing and Mandalay** **Pyin Oo Lwin (8 Individual**: 1 computer training centre, 2 fiber company, 1 Internet service provider, 2 phone shops, 1 tower company, 1 tower sub-contractor) **Mandalay (8 Individual**: 1 phone shop, 3 tower Companies, 1 tower sub-contractor, 1 fiber company, 1 ICT park developer, 1 software developer) **1 FGD** (1 tower company & top-up card printing factory). **Yangon** **(11 Individual**: 1 advisory firm, 2 tower companies, 3 tower sub-contractors, 1 cybersecurity company, 1 data services, 1 enterprise software developer, 1 hardware and infrastructure, 1 startup company) **Taunggyi, Nyaung Shwe, Shwe Nyaung and Hopong** **Taunggyi (2 Individual**: 1 local business, 1 tower sub-contractor) **Nyaung Shwe (3 Individual**: 1 Internet shop, 1 local business, 1 software developer) **Thaton, Mawlamyine, Hpa-An, Kawkareik, Myawaddy** **Thaton (2 Individual**: 1 security service provider, 1

	telecommunications operator sub-contractor) **Mawlamyine (1 Individual** : tower sub- contractor) **Hpa-An (3 Individual**: 2 tower sub-contractors, 1 local business) **Myawaddy (4 Individual**: 1 bank, 1 network company, 1 phone shop, 1 tower sub-contractor / **1 FGD**: 1 fiber company)
Community 38 Individual interviews 8 Focus group discussions (FGD) 48 Male 26 Female	**<u>Pyin Oo Lwin, Sagaing and Mandalay</u>** **Pyin Oo Lwin (2 Individuals**: 1 land owner, 1 religious leader) **Sagaing (1 Individual**: Land owner) **Mandalay (7 Individuals**: 3 land owners, 3 neighbours of land owners hosting ICT towers, 1 school assistant) **<u>Yangon</u>** **(4 Individuals:** 1 land owner, 1 religious leader, 2 neighbour) **<u>Taunggyi, Nyaung Shwe, Shwe Nyaung and Hopong</u>** **Taunggyi (7 Individuals**: 2 land owners, 2 villagers, 1 village elder, 1 village leader, 1 IT Developer / **5 FGDs**: 1 male student FGD, 1 female student FGD, 2 male villager FGD, 1 female villager FGD) **Hopong (1 Individual:** 1 Villager) **<u>Thaton, Mawlamyine, Hpa-An, Myawaddy</u>** **Thaton (4 Individual**: 1 land owner, 3 neighbours / **1 FGD**: 1 neighbour of land owner hosting an ICT tower) **Mawlamyine (3 Individual**: 1 land owner, 1 neighbour, 1 Muslim community member) **Hpa-An (7 Individual:** 2 religious leaders, 2 village administrator, 3 villagers) **Myawaddy (2 Individual**: 2 villagers / **2 FGD**: 1 village leader, 1 migrant worker)
CBO/NGO/UN 23 Individual interviews 7 Focus group discussions (FGD) 52 Male 21 Female	**<u>Pyin Oo Lwin, Sagaing and Mandalay</u>** **Mandalay (5 FGD:** 4 rights-based focused, 1 IT focused) **<u>Yangon</u>** **6 Individual** (2 IT focused, 1 gender, 1 development, 1 rights based, 1 incubator hub) **<u>Taunggyi, Nyaung Shwe, Shwe Nyaung and Hopong</u>** **Taunggyi (6 Individual:** 2 CBO, 3 LNGO, 1 LNGO) **Nyaung Shwe (1 Individual**: 1 LNGO) **<u>Thaton, Mawlamyine, Hpa-An, Myawaddy</u>** **Thaton (1 FGD:** 1 FGD with community based organisations (CBO) and local NGO (LNGO) working on health care) **Mawlamyine (1 Individual:** 1 LNGO) **Hpa-An (5 Individual:** 2 LNGO, 2 international NGO (INGO), 1 UN / **1 FGD:** 1 CBO) **Myawaddy (4 Individual**: 1 CBO, 2 NGO, 1 UN)
Government 17 Individual interviews 1 Focus group discussion (FGD)	**<u>Pyin Oo Lwin, Sagaing and Mandalay</u>** **Pyin Oo Lwin (3 Individual)** **Mandalay (3 Individual/ 1 FGD)**

20 Male 5 Female	**<u>Yangon</u> (1 Individual)** **<u>Taunggyi, Nyaung Shwe, Shwe Nyaung and Hopong</u>** **Taunggyi (3 Individual)** **Nyaung Shwe (1 Individual)** **<u>Thaton, Mawlamyine, Hpa-An, Myawaddy</u>** **Thaton (1 individual)** **Mawlamyine (2 individual)** **Hpa-An (2 individual**) **Myawaddy (1 individual)**
Media 7 Individual interviews 1 Focus group discussion (FGD) 12 Male	**<u>Pyin Oo Lwin, Sagaing and Mandalay</u>** **Mandalay (1 FGD**) **<u>Yangon</u>** **(7 individual)**
Political Party 5 Individual interviews 3 Focus group discussions 14 Male 5 Female	**<u>Taunggyi, Nyaung Shwe, Shwe Nyaung and Hopong</u>** **Taunggyi (3 FGD)** **<u>Thaton, Mawlamyine, Hpa-An, Myawaddy</u>** **Hpa-An (1 individual)** **<u>Yangon</u>** **(4 individual)**
University 5 Individual interviews 6 Focus group discussions (FGD) 20 Male 24 Female	**<u>Pyin Oo Lwin, Sagaing and Mandalay</u>** **Pyin Oo Lwin (1 Individual**: 1 professor) **<u>Yangon</u>** **(2 Individual:** 1 rector, 1 PhD Candidate / **4 FGD:** 2 male student, 1 female student, 1 professor) **<u>Taunggyi, Nyaung Shwe, Shwe Nyaung and Hopong</u>** **Taunggyi (2 Individual:** 1 rector, 1 military professor / **2 FGD:** 1 student, 1 professor)
Worker 4 Individual interviews 9 Focus group discussions (FGD) 44 Male 20 Female	**<u>Pyin Oo Lwin, Sagaing and Mandalay</u>** **Pyin Oo Lwin (2 Individual**: 1 tower company sub-contractor, 1 fiber company / **3 FGD**: 1 tower company, 1 tower company sub-contractor, 1 fiber company) **Mandalay (2 FGD**: 1 male, 1 female) **<u>Yangon</u>** **(2 FGD**: 1 male worker, 1 female worker) **<u>Taunggyi, Nyaung Shwe, Shwe Nyaung and Hopong</u>** **Taunggyi (1 Individual**: Head of workers/ **1 FGD**: 1 fiber company) **<u>Thaton, Mawlamyine, Hpa-An, Myawaddy</u>** **Myawaddy (1 Individual**: 1 spouse of lead worker / **1 FGD:** 1 spouse of worker)

Annex A

The ICT SWIA Field Research Team

One of the objectives of the SWIA programme is to build the capacity of Myanmar researchers to understand human rights issues and their connection to business and to begin to develop researchers in Myanmar with this skill set. The intention was to equip the researchers to participate in assessing and contributing to consultations on issues of responsible business following their work with MCRB.

The ICT SWIA team consisted of a Myanmar SWIA manager (responsible for several current and future SWIA processes in Myanmar), an ICT Research Leader and two field researchers. The Research Leader was an ICT sector expert and the field researchers had a background in conducting qualitative and quantitative social science research. All field staff received thorough training before visiting the field. The training was carried out by local and international experts, covering basic human rights and business training, an introduction to the practice of social impact assessment, sessions on human rights impacts of the ICT sector, sessions on how to conduct focus group discussions, ethical standards for conducting field research, labour unions, foreign direct investment, and an introduction to the various SWIA questionnaires and desk research.

Following the first round of field visits, IHRB and DIHR experts debriefed the team in Yangon to reflect on the team's findings and fine-tune the research approach and the subsequent data compilation process. Following the final field visits, all the researchers' written interview notes were translated from Burmese to English. IHRB then synthesised the data to compile the field research findings for the report and held several discussions with the SWIA Manager and Research Leader to ensure the findings were accurately reported and root causes analysed.

ICT Field Researchers in Sagaing, Myanmar (Dec. 2014)

The Myanmar Centre for Responsible Business (MCRB) was set up in 2013 by the Institute for Human Rights and Business (IHRB) and the Danish Institute for Human Rights (DIHR) with funding from several donor governments. Based in Yangon, it aims to provide a trusted and impartial platform for the creation of knowledge, capacity, and dialogue amongst businesses, civil society organisations (CSO) and governments to encourage responsible business conduct throughout Myanmar. Responsible business means business conduct that works for the long-term interests of Myanmar and its people, based on responsible social and environmental performance within the context of international standards

Myanmar Centre for Responsible Business
15 Shan Yeiktha Street
Sanchaung, Yangon, Myanmar
Email: info@myanmar-responsiblebusiness.org
Web: www.myanmar-responsiblebusiness.org
or www.mcrb.org.mm

Institute for Human Rights and Business (IHRB)
34b York Way
London, N1 9AB
United Kingdom
Email: info@ihrb.org
Web: www.ihrb.org

Danish Institute for Human Rights (DIHR)
Wilders Plads 8K
1403 Copenhagen K
Email: info@humanrights.dk
Web: www.humanrights.dk