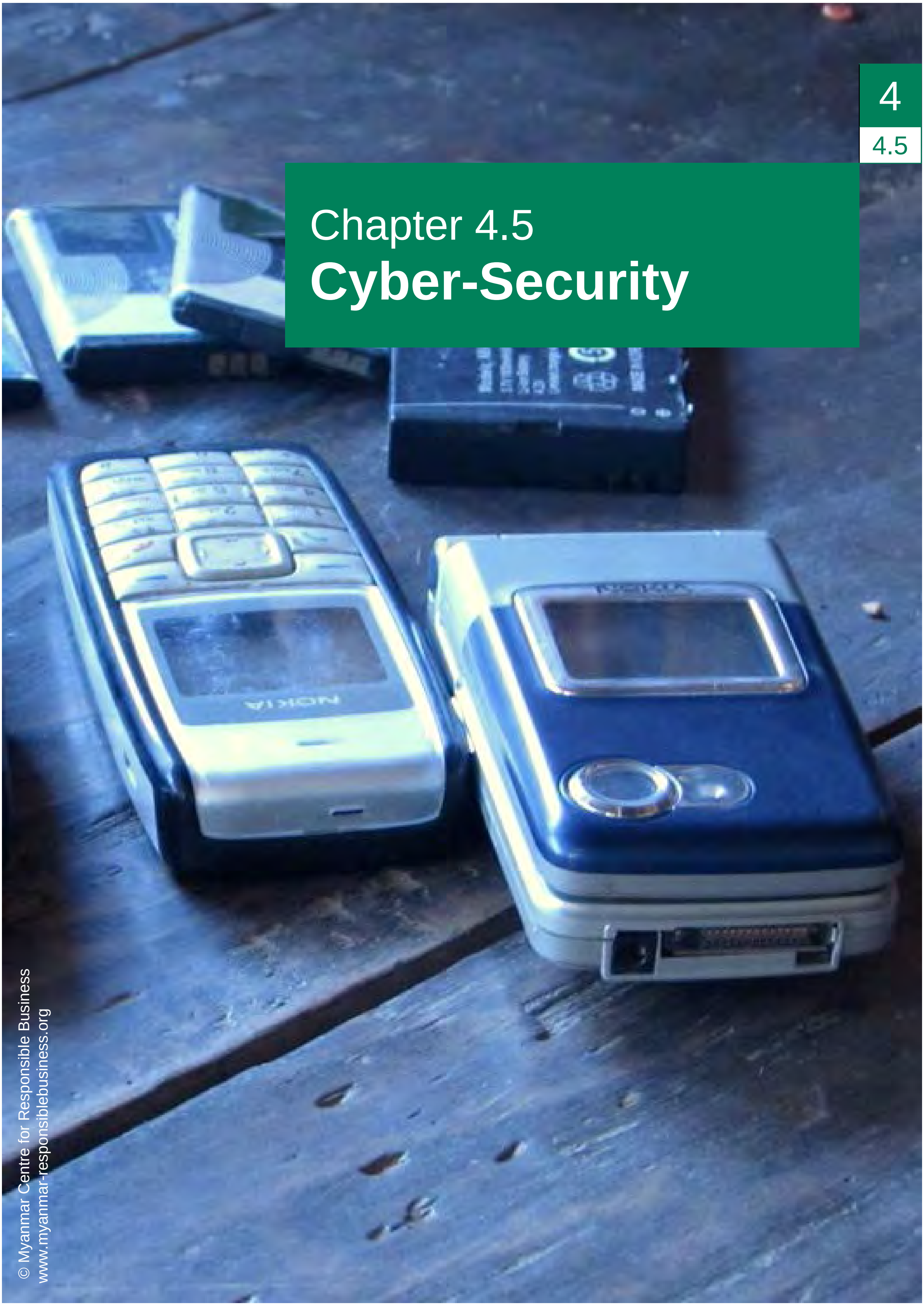
Chapter 4.5
Cyber-Security



Chapter 4.5
Cybersecurity

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.

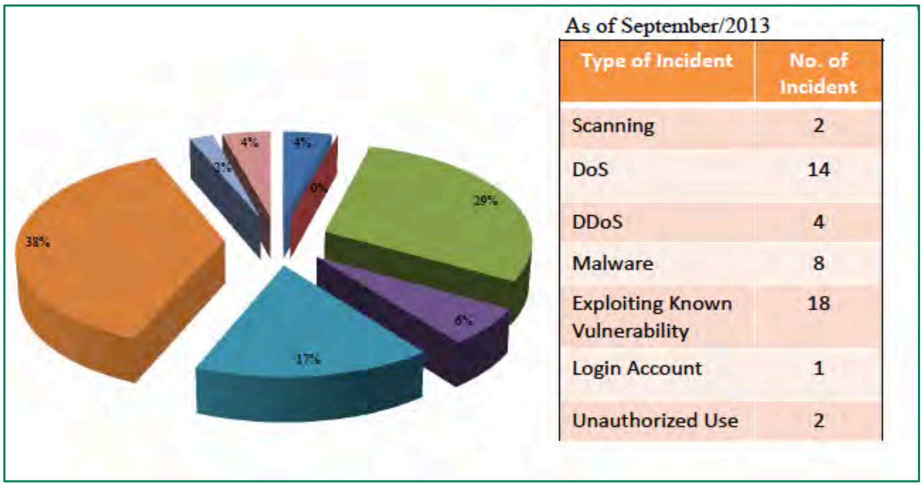
However some governments are already specifically targeting civil society groups because they use encryption and Internet security techniques. One of the charges against the jailed Zone 9 bloggers in Ethiopia is their use of encrypted communication and participating in trainings on Internet security.[417] 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.

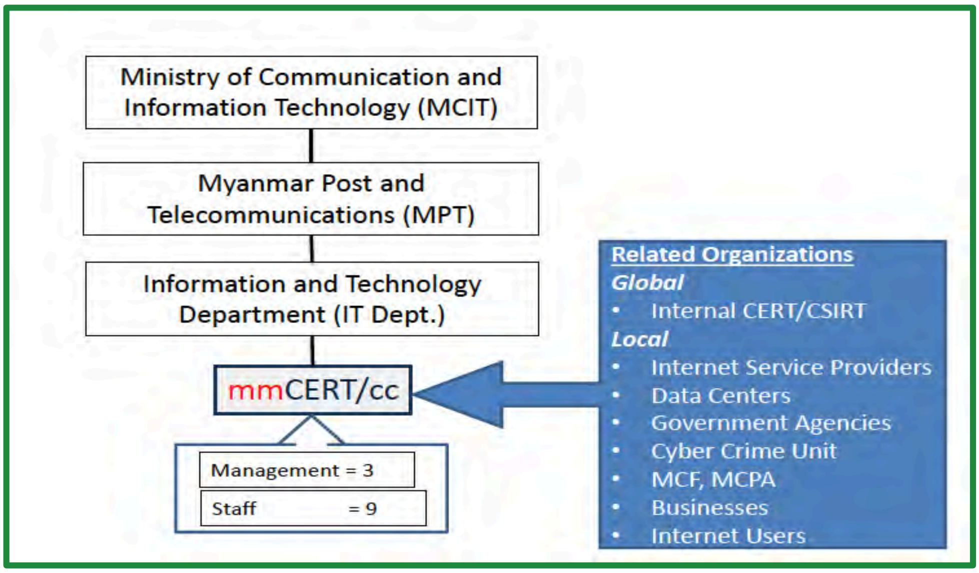
[426] Myanmar *Electronic Transactions Law.*
427 Htun Htun Minn, "Microsoft Tapped To Assist Myanmar Develop Cyber Security Measures" *Myanmar Business Today* (24 June 2014).
[428] See, Ministry of Communications and Information Technology, "The Follow-Up Project of the Establishment of an ICT Master 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


Ministry of Communication and Information Technology (MCIT)
Myanmar Post and Telecommunications (MPT)
Information and Technology Department (IT Dept.)
mmCERT/cc
Management = 3
Staff = 9
Related Organizations
Global
Internal CERT/CSIRT
Local
Internet Service Providers
Data Centers
Government Agencies
Cyber Crime Unit
MCF, MCPA
Businesses
Internet Users

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).