Myanmar Centre for Responsible Business

POLICY BRIEF
CYBER SECURITY AND CYBER CRIME: ISSUES FOR MYANMAR

This Policy Brief[1] provides an overview of terminology, concepts and good and bad practices in addressing **cyber security** and **cyber crime.** These terms are widely used but often poorly understood. The Brief aims to contribute to a more informed discussion in Myanmar on these topics.

Attacks on networks and devices within Myanmar appear to be on the rise, as they are globally. However, Myanmar does not currently have in place an overall cyber security framework, nor specific laws for cyber crime or data protection.

The Policy Brief aims to support the Myanmar Government, the private sector and civil society to fill the gaps in Myanmar's policy and legal framework and establish cyber security framework(s) and cyber crime law(s) that protect both security and human rights. This is necessary for the digital ecosystem in Myanmar to thrive. Filling these legal gaps needs to be done in a way which protects human rights since this builds trust for users. As a recent World Bank Cyber Toolkit notes, "*it is well understood that "trust" in the use of the internet and ICTs will engender use, and that part of building this trust environment in cyberspace involves striking a balance between establishing the security of networks, devices and data, and ensuring that fundamental rights such as privacy (including data protection) and freedom of expression are observed*."[2]

CYBER SECURITY OR CYBER CRIME?

Cyber security and cyber crime are not the same. They therefore should be dealt with separately, using targeted approaches for each area, rather than trying to deal with all issues in one law.

- **Cyber security** refers to a **technical approach** to securing computer systems from attack and failure. Computer systems are complex and are likely to contain flaws that affect the security of those systems. Good cyber security recognises that computer systems contain vulnerabilities and prioritises identification and fixing vulnerabilities.[3]
- **Cyber crime** refers to a criminal law approach to punish unauthorised access to computer systems, carried out with criminal intent to damage or alter the systems or the data on it, and to punish specified criminal acts carried out using computer systems. Criminal law is used both to punish and to deter.

Cyber security should be **treated as a public good**. The Government's approach to cyber security can be compared to its approach to public health: it is a collective responsibility that is for the benefit of everyone. The core obligation is on the Government to establish an appropriate cyber security framework and ensure it is implemented.

It is impossible to prevent all cyber attacks. Systems are inherently vulnerable and it is likely that systems will suffer some degree of attack at some point. **Preventing attacks as much as possible** is important. But good cyber security also requires **resilience.** Resilience means being able to effectively

[1] With thanks to Privacy International. This Briefing Paper draws on information featured in Privacy International's : *After the Gold Rush: Developing Cyber Security Frameworks and Cyber Crime Legislation to Safeguard Privacy and Security* (September 2018)

[2] World Bank and United Nations (2017). *Combatting Cybercrime: Tools and Capacity Building for Emerging Economies*, Washington, DC., p. 18

[3] More resources from Privacy International on cyber security: https://privacyinternational.org/topics/cyber-security

recover from an attack without loss of data or permanent damage to a system.

SIX ACTIONS TO INCREASE CYBER SECURITY

1. Establish a cyber security framework rather than one law in isolation

Cyber security is made up of different, complementary initiatives and approaches. Laws are just one element. Other, non-legal mechanisms include minimum standards of security, investment in security research, and security audits of key industries and public bodies. Clear and consistent frameworks, strategies and policies – such as a National Cyber Security Strategy – can set out standards of security while at the same time ensuring that human rights are protected.

2. Prioritise protecting and defending individuals, devices, and networks as the core objective of any cyber security strategy / policy

Good cyber security policies and practices put people and their rights at the centre and seek to strengthen and protect human rights as a core objective of the strategy.

- **Protecting Individuals:** Cyber security frameworks must include data protection laws which safeguard against the exploitation of personal data collected by companies and public bodies.
- **Protecting Devices**: Securing devices (such as routers, webcams and other household objects connected to the internet -- known as the "Internet of Things" (IoT)) should be a key cyber security objective. These devices are a risk to privacy because they generate, collect and transmit personal data that should be protected. If they are integrated into a network they are also a risk to security as they are often the weakest link in network security protection.
- **Protecting Networks:** Good network security means reducing the attack surface and allowing only the right people through the right devices to access the right services on a network -- and then keeping everyone and everything else out.

3. Adopt and implement a comprehensive data protection law

There must be legal obligations on companies and public bodies to protect personal data from: abuse, being excessively collected, poorly secured or at risk of being stolen. Myanmar currently lacks a data protection law.[4]

4. Identify and prioritise the security of the country's critical infrastructure

Critical infrastructure is largely defined as essential systems whose damage or loss would have a significant impact on the functioning of the State and the safety of the people. Each government must decide what it considers "critical", but such designated infrastructure often includes energy (electricity, oil, gas), transport (air, rail, water, road), banking & financial market infrastructure, digital infrastructure, chemicals, food, health, water, and emergency services.

5. Establish incident response teams

These teams of experts are the frontline when a security incident happens. They mostly deal with compromised devices or services that are enabling cyber attacks. Ideally, they should be independent of government departments. The most common is a Cyber Security Incident Response Team (CSIRT) which handles security incidents that involve ICT infrastructure. [5] Myanmar has the Myanmar Computer Emergency Response Team (mmCERT), a non-profit organization, for dealing with cyber security incidents.[6]

---

[4] See MCRB's companion Policy Brief on Privacy and Data Protection.

[5] FIRST, the global forum of incident response and security teams, conduct training workshops and have a lot of resources available on how to set up a CSIRT See https://www.first.org/ and slides on how to set up a CSIRT www.first.org/education/trainings

[6] https://www.mmcert.org.mm/

6. Undertake a proper threat assessment and develop recovery plans

A threat assessment considers possible weaknesses, such as outdated infrastructure, that make the country more vulnerable to attack. Once threats have been assessed, this helps allocate limited resources to tackling the most acute threats. CSIRTs can help in making these assessments.

TWO ACTIONS TO AVOID THAT DECREASE CYBER SECURITY

Certain activities do not enhance cyber security, and may decrease it:

1. Do not spend time and resources on developing offensive powers

As more daily transactions shift to online – from mobile banking to e-commerce – threats from cyber crime to the economy and national security will increase. Myanmar has limited resources and expertise to address cyber security. The resources it has should be invested in **defensive** capabilities to detect and manage threats in order to build trust in business and government services. Investing limited resources in **offensive** powers such as monitoring and surveillance equipment, rather than defensive capabilities, leaves the cyber security of individuals, devices and networks at risk.

2. Do not shroud cyber security in secrecy

A clear, accessible and comprehensive cyber security policy and law(s) should be established and debated through public consultations. Developing Myanmar's approach and its implementation in secret leaves the public and businesses at a disadvantage as they are not aware of the real threats and how they can protect themselves. Such an approach is the opposite of cyber security.

HOW SHOULD CYBER CRIME BE ADDRESSED?

While cyber security is concerned with technically securing systems, cyber crime is about deterring and punishing crimes involving computers. As cyber crime knows no borders, cross border co-operation is often required to address the crimes. A list of precisely defined cyber crimes can help, since cross-border cooperation may first require both the States to agree that the action is a crime. There is no globally accepted definition of cyber crimes. They are generally considered to include two groups of crimes that are different and therefore should be addressed separately in policy and law.

Cyber dependent crimes: These are criminal actions which can only be committed using a computer or device. They are directed against the confidentiality, integrity and availability of computer systems and networks and the data stored and processed on them. The core principle should be to punish unauthorized access with criminal intent. Examples include:

- breaking into the computer systems with the intention of harming or shutting it down
- "phishing" (fake emails that try to gain access to peoples' passwords and details)
- spreading viruses and trojans
- initiating a distributed denial of service ("DDOS") attack which can disable websites
- distributing malware which can, for example, record key strokes and steal passwords

Cyber enabled crimes: This includes a far broader list of established crimes where technology allows them to be committed in a new way. Essentially these are crimes that could be committed online or offline. Examples include:

- fraud using emails
- distribution of child abuse images
- distributing intimate images without consent (known as "revenge porn").

There are increasing concerns that some governments are seeking to identify behaviour as a 'cyber crime' just because it is carried out over the internet, even though it is not and should not be criminalized. This includes broadly worded, imprecise actions ("spreading information that offends the nation", "insulting family values," "frequently sending a large number of emails"), with or without additional requirements around criminal intent. These vaguely worded provisions can violate international human rights law because they can be misused to criminalise political opponents and

criticism of a government, jail journalists investigating corruption, censor freedom of expression, and more broadly discourage use of the internet.

THREE STEPS FOR DEVELOPING GOOD CYBER CRIME LAWS

1. **Ensure cyber crime legislation contains human rights protection and safeguards**

Cyber crime laws should be consistent with the Myanmar's international obligations to protect human rights. That should also cover provisions on accessing electronic evidence in criminal matters irrespective of the way data stored extraterritorially is accessed. The human rights principles and safeguards of legality, necessity and proportionality, prior judicial authorisation, effective oversight, notification and access to effective remedy should apply.[7]

2. **Define cyber dependent crimes narrowly**

These crimes should be interpreted to punish unauthorised access, with criminal intent, directed against the confidentiality, integrity and availability of computer systems and networks and the data stored there.

3. **Ensure comprehensive legal frameworks for "cyber enabled crime" that focus on the fundamental nature of the crime, and not only on the use of ICT**

Cyber enabled crime refers to 'traditional' crimes committed in a new way using technology, such as fraud or distribution of child abuse images which should be a crime whether or not a computer is used. Therefore these crimes should be addressed in comprehensive criminal laws where the crime can be defined more precisely; put in its broader context; and the appropriate procedures for investigating and prosecuting the crime defined in more detail.

THREE STEPS TO AVOID WHEN DEVELOPING CYBER CRIME LAWS

1. **Do not criminalise behaviour that should not be criminal under international human rights law**

Examples include criticising the government on social media or using encrypted messaging services.

2. **Do not mix surveillance together with a cyber crime law**

Surveillance can be necessary to fight crime. But it is an intrusive act and interferes with a range of human rights. Human rights law requires any surveillance to be legal, necessary and proportionate. Authorising surveillance powers in a cyber crime law leads to an expansion of the type of crimes for which surveillance is authorized, especially if the law authorizes surveillance for cyber enabled crimes. This can result in significantly greater intrusion into peoples' privacy, particularly if it is not accompanied by procedural safeguards and other human rights protections within the law itself. Myanmar currently does not have a law on lawful surveillance/interception and lacks the pre-requisites to a rights-respecting lawful surveillance regime[8] Including a data protection law that applies to public entities as well as private ones.[9]

3. **Do not just "copy and paste" the 2001 Budapest Convention into domestic law without additional human rights safeguards**

The provisions in the Budapest Convention need to be accompanied by human rights safeguards.

The Budapest Convention - Council of Europe's Convention on Cyber Crime 2001

The Council of Europe's Convention on Cyber Crime 2001 (known as the "Budapest Convention") is a

[7] https://privacyinternational.org/advocacy-briefing/660/privacy-internationals-response-european-commissions-public-consultation

[8] For a lawful interception regime that respects human rights, see Myanmar Centre for Responsible Business' "Recommendations to the Myanmar Government: Lawful Interception and Government Access to User Data: The Characteristics of a Rights-Respecting Model" in English *Sector Wide Impact Assessment of Myanmar's ICT Sector," (2015), Recommendations – Annex*, p. 35. And in Burmese

[9] See MCRB's companion Policy Brief on Privacy and Data Protection.

framework for international cooperation on cyber crime.[10] It was also intended to "serve as a guideline for any country developing comprehensive national legislation against cyber crime" but was written two decades ago. A number of countries have used it as a basis for their own laws on cyber crime.

It has three major components:

i. establishes a list of crimes that each participating nation should have on its books
ii. requires new investigative powers to investigate cyber crime
iii. provides for cross border assistance on cyber crime

The Convention was developed in Europe where countries must also adopt the European Convention of Human Rights and European data protection legislation. It is therefore assumed that the Convention will be complemented by human rights safeguards in the wider legal system. Indeed, the Convention specifies in Article 15 that it should be complemented by human rights safeguards that are equivalent to the European Convention on Human Rights and the International Covenant on Civil and Political Rights, other applicable international human rights instruments, and the principle of proportionality.[11] These safeguards do not currently exist in Myanmar's broader legal system. Therefore new Myanmar laws relating to cybersecurity and cyber crime need to incorporate these safeguards in addition to addressing the main points in the Convention.

[10] Council of Europe, *The Convention on Cyber Crime of the Council of Europe, (CETS No. 185)*, known as The Budapest Convention.

[11] Council of Europe, *Practical Guide on the use of personal data in the police sector: how to protect personal data while combatting crime,* 15 February 2018.