

Workshop on Innovation

Session 1: Digital Fraud

MALAYSIAN COMMUNICATIONS AND MULTIMEDIA COMMISSION
25 September 2025

MCMC Roles in Cyber Security



Develop and maintain **cybersecurity roadmap** for C&M industry and develop and **maintain network security regulations, policies, and standards.**



Leading **innovative research on emerging technologies**, strengthening internal and external **capabilities** through system and tool development, and **strategic partnerships** to shape a secure and resilient digital future.

Source of Power

Malaysian Communications and Multimedia Commission Act 1998

Provides for the national policy objective to ensure the information security and network reliability and integrity.

Communication and Multimedia Act 1998

Protecting against harmful online behaviour, addressing network security risks, and expanding the powers of enforcement conferred on the MCMC.

Cyber Security Act 2024

MCMC is appointed as the National Critical Information Infrastructure (NCII) Sector Lead to oversee actions required of and duties imposed on the NCII entities.



Foster **cybersecurity and regulatory excellence** in the C&M industry, creating a **secure and resilient digital environment** that serves and protects all stakeholders.



Enforce regulatory compliance among licensees to strengthen the national **cybersecurity posture** and **CNII protection** through strategic collaborations, proactive monitoring of cybersecurity risks, and by driving continuous industry compliance.

DEFINING FRAUD: INSIGHTS AND INTERPRETATION

Fraud or '**scam**' activities, whether online or offline, are subject to the jurisdiction of the Royal Malaysian Police (PDRM), the Ministry of Domestic Trade and Consumer Affairs (KPDN), the Securities Commission (SC), Bank Negara Malaysia (BNM) or any related agency; subject to the form of fraud committed.

Cooperation between Malaysian Communications and Multimedia Commission (MCMC) and enforcement agencies consists of:

- a) Technical assistance for further investigations
- b) Provision of Information
- c) Implementation of sanctions against any breach of the CMA 98
- d) Digital forensic analysis



OVERVIEW

TECHNICAL ASSISTANCE FOR INVESTIGATION

- Profiling and intel
- Data preservation & digital forensics

CO-REGULATION WITH TELCO AND PLATFORM PROVIDERS

- Escalation of content for review/takedown/geo-blocking (OTT)
- Industry reference for phone number blocking/suspend (Phone and SMS)

INTER-AGENCY COORDINATION & CROSS FUNCTIONAL COLLABORATION

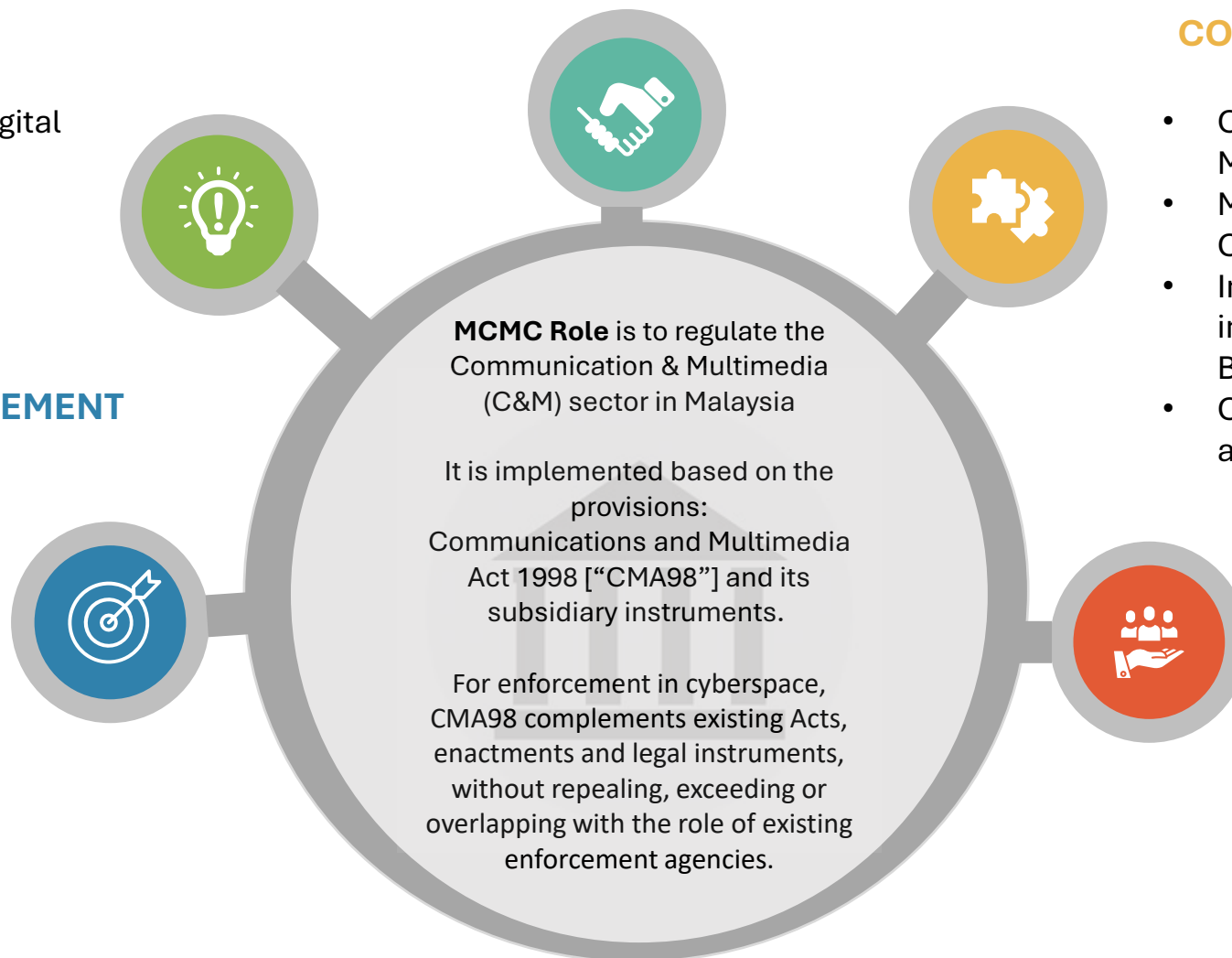
- Cybercrime Task Force (CTF) involving MCMC and PDRM.
- Member of National Scam Response Centre (NSRC).
- Internet Banking Task Force (IBTF) involving Financial Institutions and BNM.
- Collaboration with platform providers and international bodies.

USER EMPOWERMENT & ADVOCACY

- Sebenarnya.my (Fact-checking)
- Public alerts and warnings
- Awareness initiatives Kempen Internet Selamat

LEGISLATIONS & ENFORCEMENT

- Any act (that) is illegal in the physical world, will similarly be outlawed in the online environment.
 - Licencing Regime
 - Investigation
 - Access restriction
 - Phone number termination/suspension



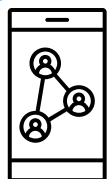
Cybercrime Mitigation

MCMC INITIATIVES - STATISTICS



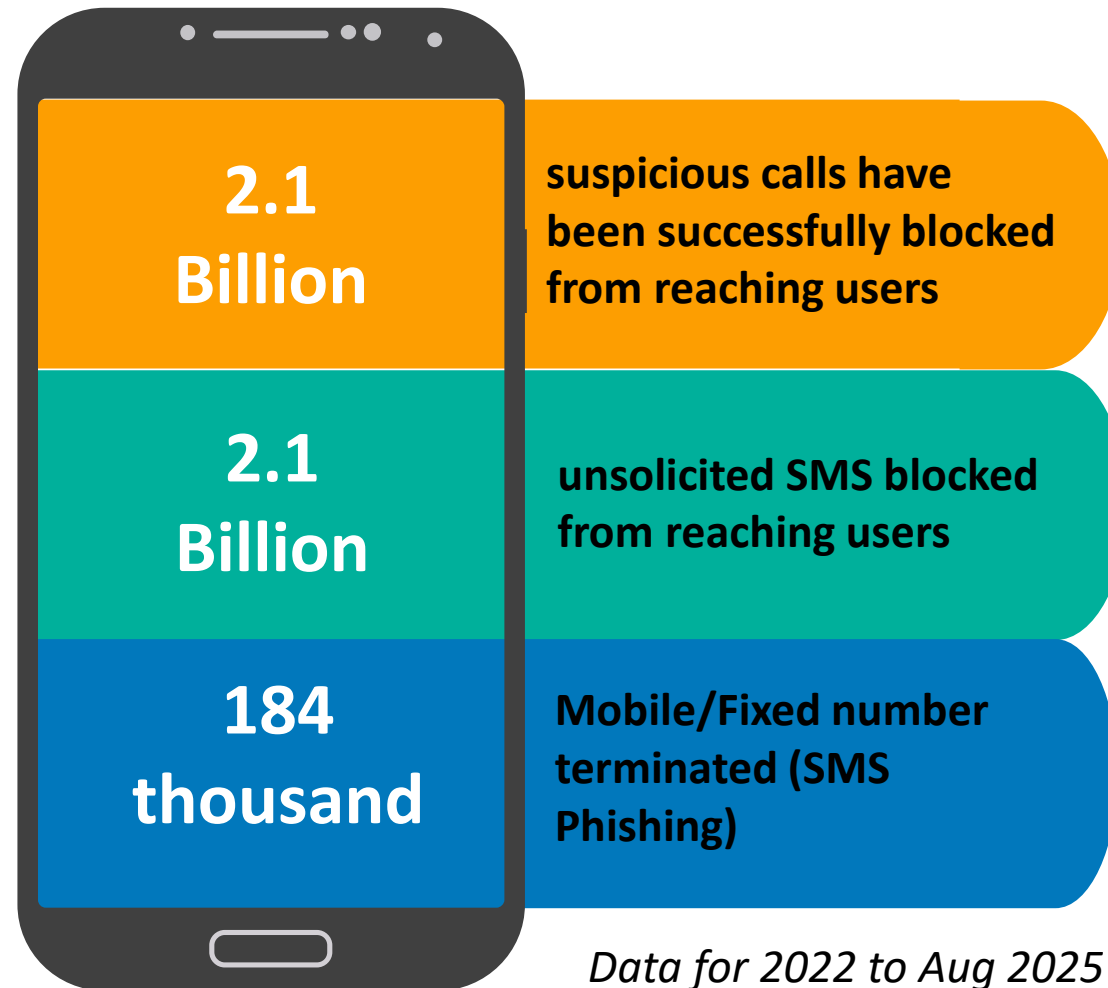
Website Blocking

- 11,648 phishing sites was blocked from year 2022 to Aug 2025



Request for account closure / content removal on social media

- 126,189 removal request submitted to social media platform provider related to scam cases from year 2022 to Aug 2025



Data for 2022 to Aug 2025

DEFINITION OF TV BOX

What is TV box?

1. Designed for **connection to television and for setup to the internet** via Wi-Fi connectivity;
2. Run on an **open-source operating system**, such as Android; and
3. Enables television to be used for **internet browsing and online contents streaming**.

Why TV box?

Consumers can **watch or stream on-demand video or audio contents on the television** using applications such as YouTube, Netflix, HBO Max Asia, Disney+, Astro Go and others.

How is it misused?

Irresponsible sellers or consumers **install illicit streaming applications** that can access and stream copyright contents illegally.

The TV box is required to be certified for its wireless modules (Bluetooth and Wi-Fi) to ensure its compliance with the technical codes (electromagnetic compatibility, interoperability, and radio frequency)



RELEVANT PROVISIONS & ACT

Sec. 232 (2), CMA 98

- Fraudulent use of network facilities, network services, etc.
- Any person who possesses, obtains or creates a system designed to fraudulently use or obtain access to content application services
- Fine $\leq$ RM300,000 or imprisonment $\leq$ 3 years or both

Reg. 16, TSR 2000

- Prohibitions of sale, etc., of communications equipment
- Users & suppliers of non-certified communications equipment
- Fine $\leq$ RM300,000 or imprisonment $\leq$ 3 years or both

Reg 23 & 24, TSR 2000

- Suspension or cancellation of compliance certificate for failure to comply with the conditions and standards (reg. 23)
- Certificate holders may be directed to recall the equipment (reg. 24)

RELEVANT PROVISION

ENFORCEMENT ACTION TAKEN FOR TV BOXES

☐ COMPLAINTS (2018 – 2025)

YEAR	FIR	STATUS				REMARKS
		NOD	Ongoing	NFA	Charged	
2018	5	2		1	2	RM 75,000
2019	4	2			2	RM 14,000
2020	5	4			1	RM 4,000
2021	3	1			2	RM 37,000
2024	5		2	2	1	RM 14,000
2025	3		3			
Total	25	9	5	3	8	RM 144,000

☐ MARKET INTELLIGENCE (2022 – 2025)

YEAR	FIR	STATUS			REMARKS
		NOD	Ongoing	Charged	
2022	4	2		2	RM 20,000
2024	2		2		
Total	6	2	2	2	RM 20,000

Summary of Actions

- **31 cases of** TV boxes are investigated by MCMC from 2018 to 2025
- Total court fines = **RM 164,000**

FAKE BASE TRANSCEIVER STATION (BTS)

What is it?

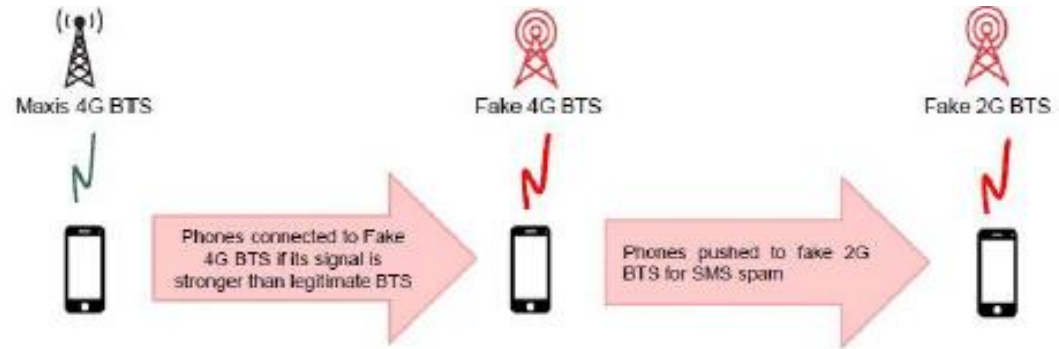
A fake Base Transceiver Station (BTS) is an unauthorized, rogue cellular tower that imitates a legitimate mobile network (e.g., 2G/4G) to covertly engage with nearby mobile devices. It is also known as an IMSI catcher, Stingray, or Rogue BTS.

How does fake BTS work?

- Broadcasts a stronger signal than nearby legitimate towers to lure mobile devices.
- Exploits vulnerabilities in mobile network protocols (especially 2G) to:
 - ✓ Capture device identifiers (IMSI, IMEI)
 - ✓ Intercept voice calls and SMS
 - ✓ Track device location
 - ✓ Inject malicious messages (e.g., SMS phishing)

Type of fake BTS

- Fixed – transmitter installed from a building
- Mobile – transmitter install in a vehicle / in travel luggage at public area



What is the impact?

- Poor signal quality – degradation of quality and internet speed.
- Theft of personal data – IMSI details of user leaked
- Fake / scam SMS – linked to syndicate operation for monetization

OTHER MEASURES – FAKE BTS MITIGATION



Stationary Fake BTS: Brickfields



AirBnB Premise – No occupant, devices operated remotely.
Fake/no tenant credentials.

Fan / aircond constantly turned on for device cooling.



OTHER MEASURES – FAKE BTS MITIGATION



In-vehicle Fake BTS



OTHER MEASURES – FAKE BTS MITIGATION



In-vehicle Fake BTS

A video player showing a scene from inside a car. A police officer in a dark uniform is standing outside the car, looking into the open driver's side door. The driver is seated, and the officer appears to be inspecting something in the car. The video player has a progress bar at the bottom showing 0:18 / 1:38.

Suruhanjaya Komunikasi dan Multimedia Malaysia [Follow](#)

6 September at 09:13 · [Public](#)

MCMC bersama Polis Diraja Malaysia (PDRM) menumpaskan sindiket SMS palsu menggunakan peralatan haram Fake Base Transceiver Station (Fake BTS) dalam Op Pancing baru-baru ini. Seorang individu ditahan di Kuala Lumpur ketika mengendalikan peralatan aktif yang menghantar SMS palsu, pautan phishing dan mesej perjudian.

Serbuan susulan di Kota Kemuning, Shah Alam menemukan 45 barangan termasuk sebuah kenderaan pelbagai guna (MPV) dan kelengkapan komunikasi bernilai kira-kira RM100,000.

Kes disiasat di bawah Akta Komunikasi dan Multimedia 1998 serta Peraturan-Peraturan Spektrum 2000, dengan hukuman denda sehingga RM1 juta atau penjara maksimum 10 tahun. MCMC akan terus bekerjasama dengan Polis Diraja Malaysia membanteras jenayah komunikasi demi keselamatan rakyat.

[See less](#)

[Comment](#) Suruhanjaya Komunikasi dan Multimedia Malaysia limited who can comment on this post.

<https://www.facebook.com/SuruhanjayaKomunikasiMultimediaMalaysia/videos/mcmc-bersama-polis-diraja-malaysia-pdrm-menumpaskan-sindiket-sms-palsu-menggunak/1090561859959857/>

National Scam Response Centre (NSRC)



National Scam Response Centre (NSRC), is a one-stop operations center combining the expertise of the Royal Malaysia Police (PDRM), Bank Negara Malaysia (BNM), **MCMC**, and the National Financial Crime Prevention Centre (NFCC).

This initiative aims to ensure swift and effective action in combating cyber fraud through the following methods:

1

Complaint management and immediate action against reported scam.

2

Integrated enforcement actions against scam.

3

National-level coordination for scam awareness and prevention.

NSRC – Roles of Collaborating Agencies



- ❖ Conduct joint analysis of data/information.
- ❖ Coordinate enforcement actions for integrated operations.
- ❖ Streamline the management of seized assets for the cases involved



- ❖ Receive police reports from fraud victims.
- ❖ Conduct investigations, freeze, and seize suspected accounts.
- ❖ Lead integrated operations in collaboration with other enforcement agencies



- ❖ Provide immediate information to banking institutions for prompt detection and action.
- ❖ Circuit breaking.
- ❖ Conduct financial intelligence analysis on syndicates suspected of involvement.



- ❖ Coordinate immediate action with Telcos.
- ❖ Conduct intelligence analysis to track phone numbers and their locations.
- ❖ Block and terminate phone number services, and block spoofed traffic at gateways.

Managing Misinformation and Disinformation



Awareness Campaign



Objective: Foster **positive values** & enhance **online safety** for children & families

Launched: 21 Jan 2025, Kota Bharu, Kelantan

Target Audience: Educators, Children (U13), Parents, Elderly, Social Media Providers, NGOs

Focus Areas:
Cyberbullying | Fake News | Age Limit for Social Media | Online Gambling



Outreach	
Nationwide Campaign 2025 until 2027:	Through TV, Radio, Social Media, Outdoor Media
MCMC Promotions:	Websites, Apps, Social Media



Media Plan

Raise Awareness for Ages 7-15, Parents, Educators

Through:-

- i. Social media: FB, IG, TikTok, YouTube
- ii. TV Stations: RTM, TV3, Astro, BernamaTV
- iii. Radio Stations: Era, HotFM, SinarFM, Bernama Radio
- v. News & magazine
- iv. Outdoor media: billboard, transportation wraps

Train-the-Trainers (May 2025):

To combat Online Crimes & Fake News

Focuses:

- i. Social media age limit for U13 and below
- ii. Parental supervision
- iii. Ethical Internet use

Campaign Target:

10,000 schools & all public universities

Artificial Intelligence Fact-check Assistant (AIFA) - Overview



Launched

MCMC launched AIFA on 28 January 2025.

01

Initiative

Chatbot assistant through the **Sebenarnya.my** portal and WhatsApp.

02

How it Works

- Utilizes AI technology
- Serves as an assistant to verify facts based on credible sources.

03

Accessibility

- Providing 24/7 instant verification.
- Fostering an informed society.

04

THANK YOU