emergecyber

ICT & CYBERSECURITY WORKSHOP

02 to 03 June 2026 | Emperors Palace, Gauteng

SECURING THE DIGITAL STATE

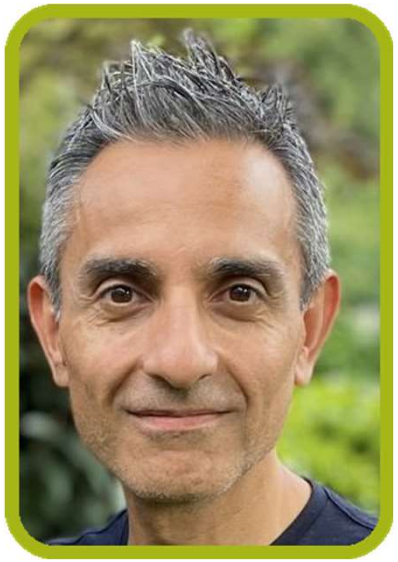
Cross-Border Collaboration in Combating Cybercrime

Advancing cyber resilience in the public sector

Jow Arif Director, EmergeCyber

CIGFARO & SAICA

About the speaker



Jow Arif

Director, EmergeCyber

Jow leads EmergeCyber, a cyber risk management firm that helps organisations find and fix the cyber risks that actually matter.

His work centres on continuous cyber risk management, an ongoing programme rather than a one-off snapshot, across businesses, charities and sports bodies.

He works with leaders and Boards to put cyber risk where decisions get made, and to fix the exploits a real attacker would use before they get the chance.

Marathon runner. Powered by double espresso.

THE STARTING POINT

South Africa signed the world's first global treaty against cybercrime.

October 2025

Hanoi, Vietnam

The first comprehensive global treaty to combat cybercrime, adopted by the UN General Assembly in December 2024.

And it did not just sign. South Africa co-chaired the United Nations expert group whose work laid the treaty's foundation.

On paper, cross-border cooperation just took its biggest step ever.

Sources: UNODC; South Africa Department of Justice and Constitutional Development, 2025

But a treaty does not stop Monday's breach

ON PAPER

Diplomacy is advancing.

Global and regional frameworks now exist to share evidence and pursue criminals across borders.

ON THE GROUND

Reality is slower.

If a public body is hit today, none of it yet catches the attacker or recovers the money.

That gap, between the diplomacy and the day job, is what this session is about.

Borders stop you, not them

A single attack on a public sector body routinely spans several countries within minutes:

1

The victim

A municipality, department or agency

>

2

The infrastructure

Servers and relays in other jurisdictions

>

3

The attacker

Often a continent away

>

4

The proceeds

Laundered through crypto across borders

Your authority ends at the border. The crime does not.

The cooperation toolkit is real, but not yet operational

Where South Africa sits on the three frameworks that matter

Budapest Convention

2001

Signed in 2001, never ratified. South Africa is not a party.

AU Malabo Convention

2014

In force since 2023, but South Africa has not ratified it, citing compatibility with existing national law. None of Africa's larger states have ratified.

UN Cybercrime Convention

2025

Shaped and signed by South Africa in Hanoi. Not yet in force.

86% of African countries say their cross-border cooperation capacity needs improvement, citing slow formal processes and limited access to foreign-hosted data.

Interpol, Africa Cyberthreat Assessment, 2025

Operation Serengeti 2.0

WHAT GOOD LOOKS LIKE | AN INTERPOL-COORDINATED CRACKDOWN, JUNE TO AUGUST 2025

18 African nations and the United Kingdom

worked together under the African Joint Operation against Cybercrime, funded by the UK Foreign, Commonwealth and Development Office.

It targeted ransomware, business email compromise, online fraud and illegal crypto mining, the threats that move fastest across borders.

South Africa was a participating country.

Source: Interpol, August 2025

Serengeti 2.0, by the numbers

1,209	$97.4M	11,432	~88,000
arrests	recovered	infrastructures dismantled	victims protected

Numbers no single country could have reached alone. That is the value of cooperation, made concrete.

Source: Interpol, August 2025 snapshot

Why it worked, and what to copy

Information sharing

Intelligence flowed in real time across 18 nations and the UK, not held inside silos.

Public-private partnership

Threat intelligence from private sector partners gave investigators the leads to act on.

Capacity building

Investigators were trained first, in open-source intelligence, crypto tracing and ransomware analysis.

The same three moves work at the scale of a single organisation.

What is coming next

The cross-border threats public bodies must prepare for

Business email compromise	Ransomware-as-a-service	Cryptocurrency laundering	**AI-enabled fraud**

Interpol's 2025 assessment flags AI-enabled fraud as the emerging danger.

These threats rise exponentially. No single control keeps pace with them. The response is not one more tool, it is a continuously rising standard.

The lever you actually control: raise your own standard

A GLOBAL PROBLEM

Even well-funded organisations carry the same gaps.

The root cause is rarely budget. It is leadership commitment: treating cyber risk as seriously as a threat profile that is rising exponentially.

THE PRACTICAL PATH

- **Align.** to a recognised framework that fits you
- **Adopt the principles first.** certification can follow later
- **Get onto the path.** that is the win, not perfection

The cross-border payoff: raise your own bar and you lift your suppliers, stop being the weak link, and give agencies and neighbouring countries something to share, what worked and what did not. Bottom-up cooperation meeting top-down.

Frameworks to build on

You do not need all of these. Pick what fits, adopt the principles, and let certification follow.

ISO/IEC 27001

Information security baseline

The global standard for managing information security as a system.

ISO/IEC 42001

The AI layer

The first AI management system standard, the partner to 27001 for the AI era.

NIST Cybersecurity Framework

Flexible and governance-led

Outcome-based and widely used, strong for Board and leadership conversations.

Cyber Essentials

An accessible on-ramp

An example of a low-barrier baseline of fundamental controls. Equivalents exist.

Aligning to common, recognised standards is itself a quiet form of the cross-border harmonisation the treaties are reaching for.

What to do, by role

Raising the standard looks different depending on where you sit

Practitioners

- Rehearse incident response
- Preserve evidence so a cross-border request can succeed
- Know where your data and processors physically sit
- Adopt the principles of a recognised framework

Regulators & policy makers

- Move frameworks from signed to in force
- Mandate incident reporting and information sharing
- Create channels to share what works across agencies

Leadership & boards

- Treat resilience as the part you control
- Commit to a rising standard, not a one-off fix
- Invest before the incident, recovery is rare

Three things to take back

1. **Cooperation is real, but slow.** Treaties and operations work, but they will not catch tomorrow's attacker for you. Do not wait on them.

2. **The model is proven.** Information sharing, partnership and capacity building delivered Serengeti. The same moves scale down to you.

3. **Raise your own standard.** It is the lever you control, and doing it makes you part of the cross-border solution rather than waiting on it.

Securing the digital state starts with what you do before the breach.

Thank you

Questions and discussion welcome

Jow Arif | Director, EmergeCyber

+44 (0)7939 176 610

jow.arif@emergecyber.com

emergecyber.com

linkedin.com/in/jow-arif-8a6688b