2026-06-03

AI-driven cyberattacks and defence mechanisms

CIGFARO
Chartered Institute of
Government Finance, Audit & Risk Officers

Norman Nhliziyo

The battlefield

CIGFARO
Chartered Institute of
Government Finance, Audit & Risk Officers

Cybersecurity reality

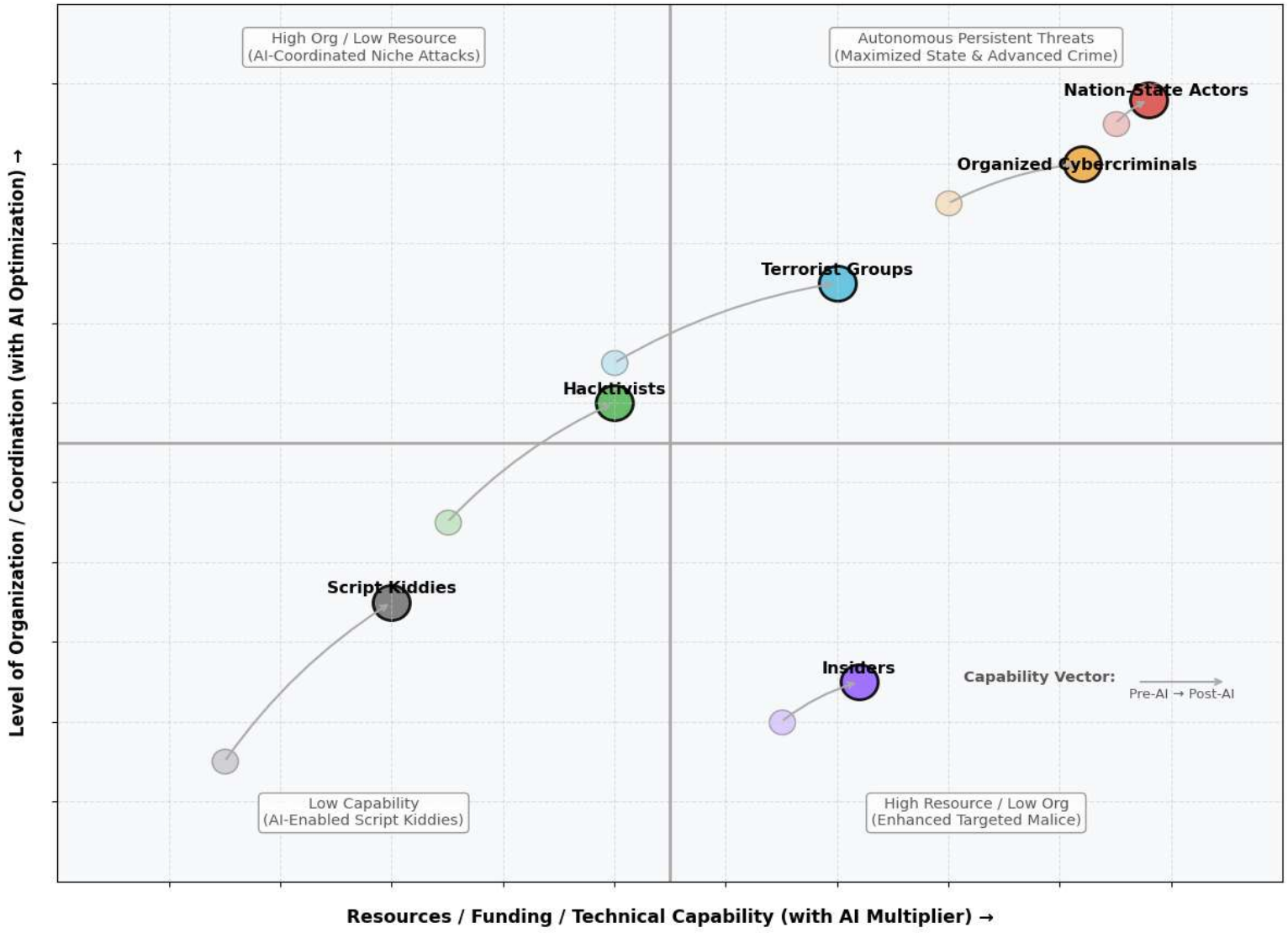
No organisation can consistently defend against an adversary whose resources, and capabilities significantly exceed its own.

Cyber adversary landscape: organisation vs resources before AI

CIGFARO
Chartered Institute of Government Finance, Audit & Risk Officers

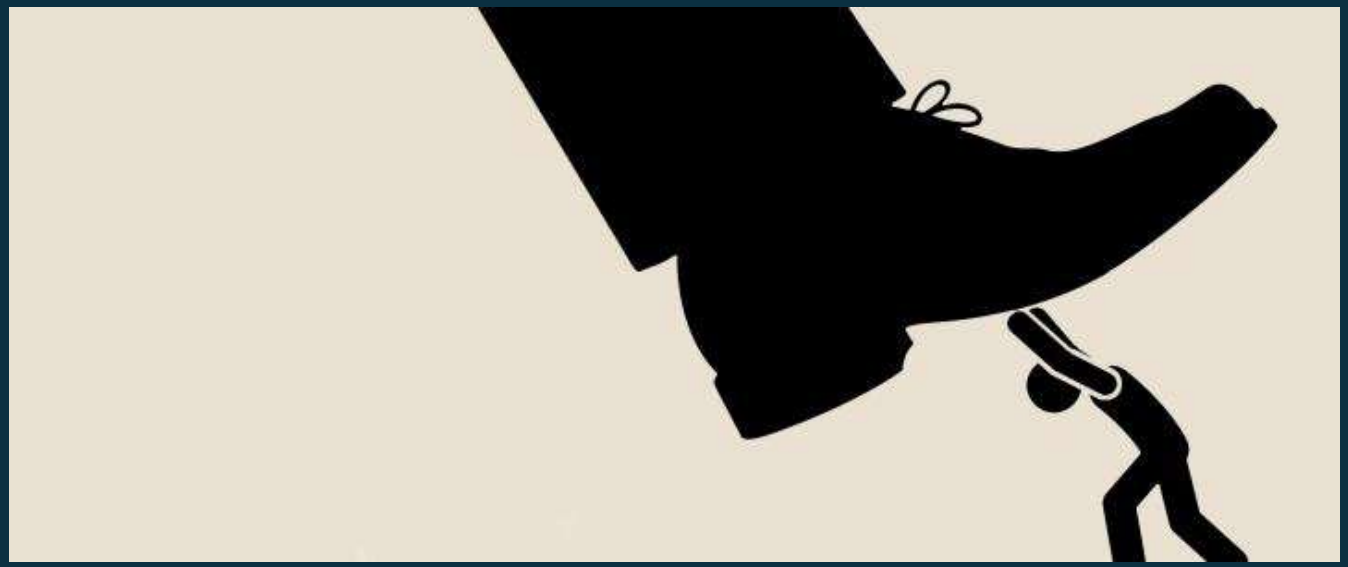
Cyber adversary landscape: organisation vs resources in the AI-era

CIGFARO
Chartered Institute of Government Finance, Audit & Risk Officers



AI is a force multiplier for attackers

CIGFARO
Chartered Institute of
Government Finance, Audit & Risk Officers



So…
can defenders win?

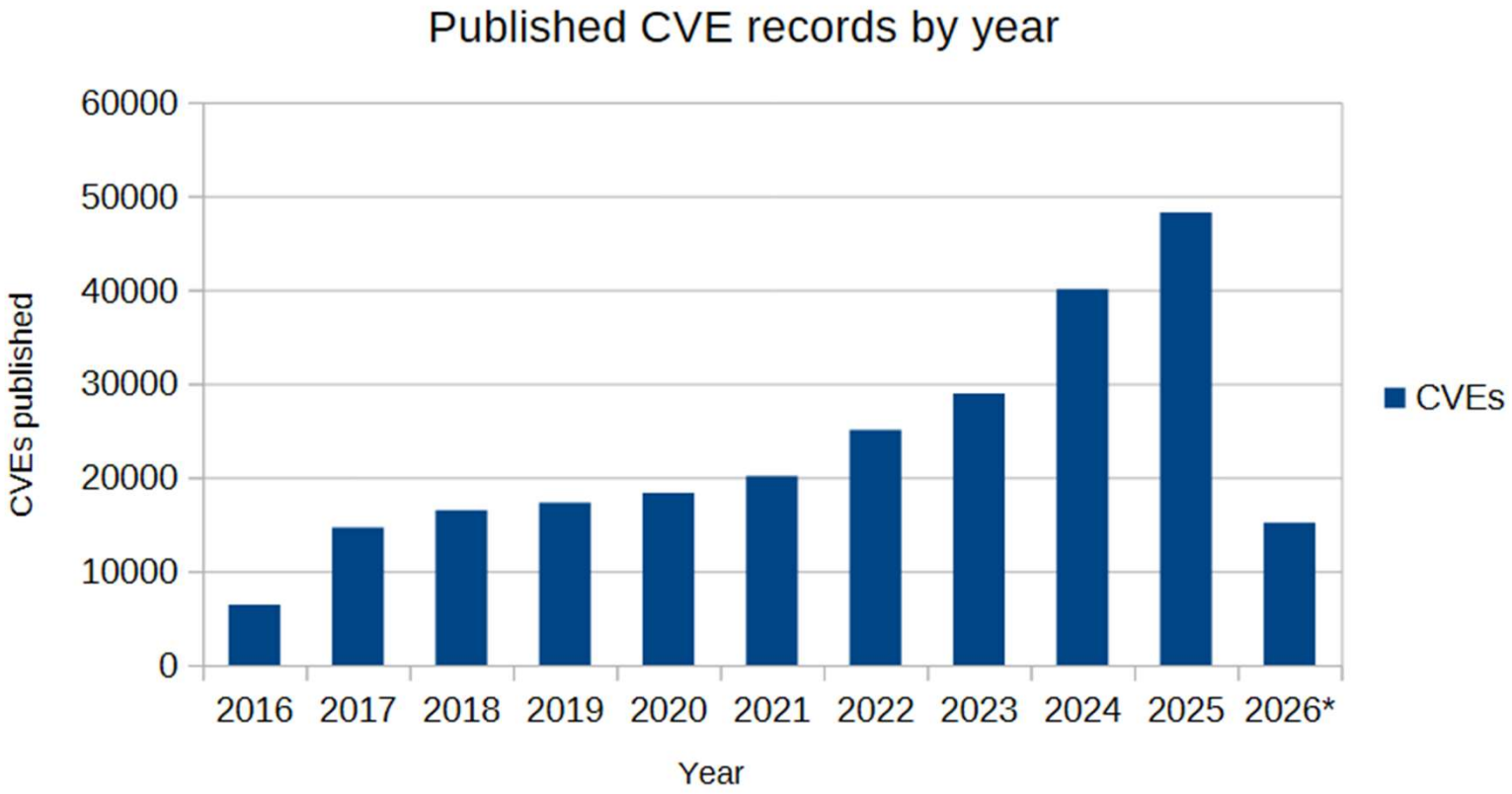
Cybersecurity professionals felt out gunned before AI. The hopelessness is real – but it is not the end of the story. We can win, and here's how.

Practical steps to manage AI threats

CIGFARO
Chartered Institute of Government Finance, Audit & Risk Officers

	Horizon 1	Horizon 2	Horizon 3
People			
Process			
Technology			

Patching, patching… patching



Monthly or quarterly patching cycles no longer cut it, and are risky – it is much easier to create exploits and the number of vulnerabilities have increased.

Target at least a fortnightly patching cycle with a view of continuous patching.

Build your human firewall

CIGFARO
Chartered Institute of Government Finance, Audit & Risk Officers

AI-generated phishing is a different beast:

- There are no more Nigerian princes or obvious grammar mistakes.
- Attacks are now hyper-personalised – your name, role, your context
- Advanced mail filters cannot catch everything.

What to do:

- Continuous scenario-based awareness training – no annual tick box.
- Simulate AI-crafted emails internally to build muscle memory.

"90% of all cyber attacks start with phishing"...

We can help

Other essentials

3rd party risk assessments
Your systems are only as secure as the weakest links. Supplier cybersecurity programmes must be assessed

Data-loss prevention (DLP)
The information you feed LLMs will be used against you. Train staff not to upload sensitive information.

Multifactor authentication
MFA is one of the highest ROI controls you can deploy, if you haven't deploy an MFA solution today.

What about AI...?

CIGFARO
Chartered Institute of Government Finance, Audit & Risk Officers

Areas where AI tooling can be leveraged

- Zero-trust network architecture (ZTNA)
  - Trust but verify;
  - User behavioural analytics (UBA)
- DevSecOps
  - Software bill of materials (SBOM)
  - Shift-left (quality gates)
  - Logging and monitoring
- Agentic workforces

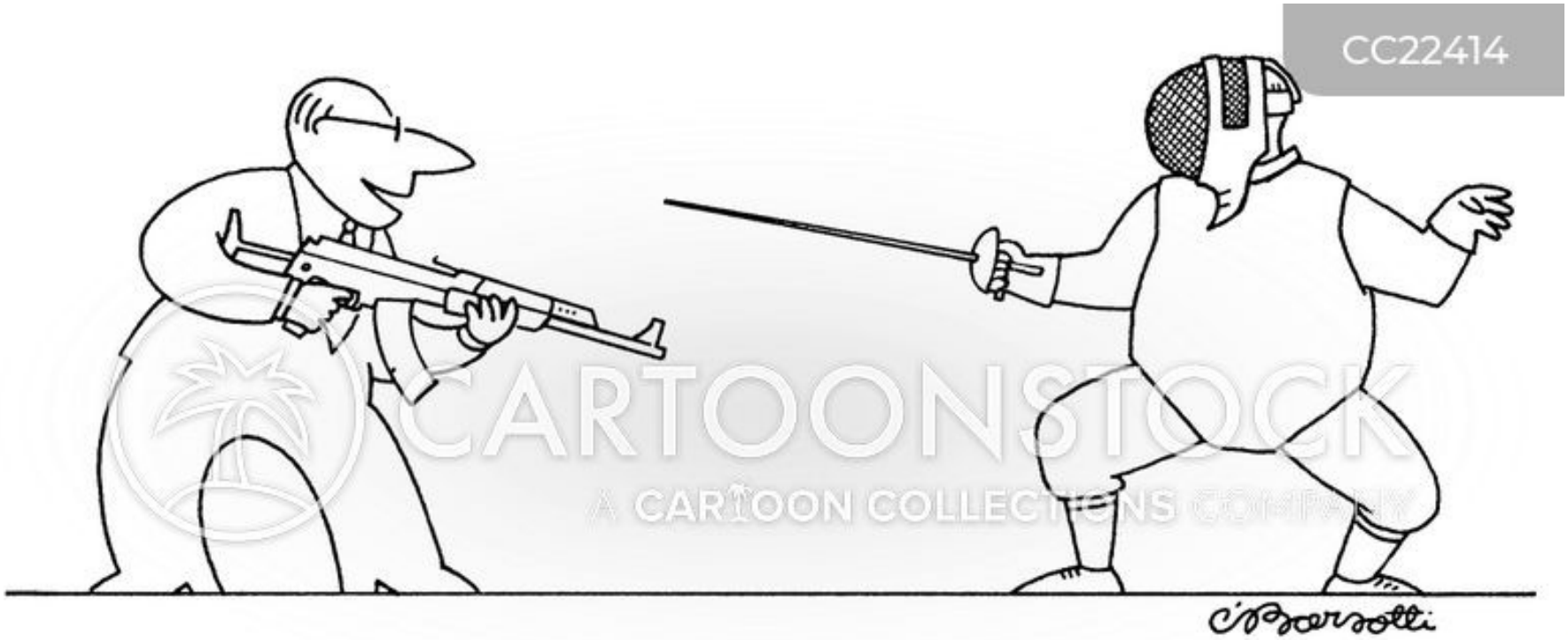
All underpinned by policies

Policies are the centrepiece of a cybersecurity strategy. They set the baseline expectations for the controls that manage cyber risk.

5 reasons why policies fail...

1. Misalignment with the business
2. Inconsistent structure
3. Wrong level of specificity
4. Written for the wrong audience
5. Poor dissemination

Conclusion: Never bring a knife to a gun fight



GROUP 19

HTTPS://GROUP19.CO.ZA
info@group19.co.za
071 923 3267

Thank You!

CIGFARO
Chartered Institute of
Government Finance, Audit & Risk Officers

www.cigfaro.co.za

SAQA Recognised Professional Body