The Central Organizing Committee of the International Conference and Advanced Workshop on Modelling and Simulation of Complex Systems

Presents

The ICAWMSCS Seminar Series

(September 2026)

Title:

Infectious Deception: An Epidemiological Blueprint for Curbing Cybercrime

DR. YUSUF OLATUNJI TIJANI

Lecturer

Affiliation:

School of Computer Science and Applied Mathematics, University of Witwatersrand, Johannesburg,

Zoom Link:
https://zoom.us/j/97592772965?pwd=i5NOuHHUa5qKWodS8g4ASLrKNviwHJ.1

Meeting ID: 975 9277 2965
Passcode: 359799

7th September, 2026

12:00 pm WAT

Infectious Deception:

An epidemiological blueprint for curbing cybercrime

Yusuf Olatunji Tijani[1,2]

[1] *School of Computer Science and Applied Mathematics, University of the Witwatersrand.*

[2] *Department of Mathematics, Rhodes University, South Africa.*

JOINT WORK WITH

Indranil Ghosh (UCD) • Shina Oloniiju (RU) • Hammed Fatoyinbo (AUT)

7 SEPTEMBER 2026

UNIVERSITY OF THE WITWATERSRAND, JOHANNESBURG

A single scam is a crime.
A population of scams is a pandemic.

Pandemics have a well-known mathematical modelling approach, one that tells us *which* intervention works and what we have to do. The SIR model!

Outlines

Why epidemiology?

PART 1 OF 7

1

Cyber-enabled fraud is a system, not a run of bad luck

Low cost, high yield

Near-zero marginal cost per extra target.

Deception at scale

One operator reaches thousands at once.

Pervasive societal cost

Financial loss, eroded trust, psychological harm.

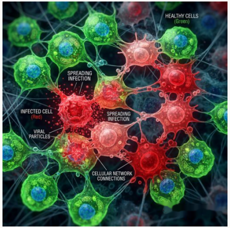
THE FRAMING

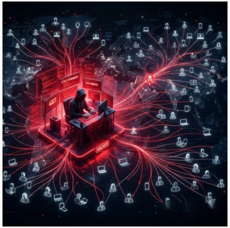
> Structurally this behaves like a **transmissible process**, not like a sequence of isolated criminal events.

The contagion paradigm

Every term in the epidemiological modelling has a cybercrime translation.

EPIDEMIOLOGY	CYBERCRIME
Infectious cell	Active scammer
Contact	Solicitation attempt
Recovered	Recovered victim
Infected	Victim
Waning immunity	Awareness that fades
Super-spreading	Automated mass outreach





> Take the analogy seriously and the whole epidemiological analysis such as equilibria, reproduction number, stability becomes available for *quantitative analysis*.

The gap this work fills

THE KNOWLEDGE GAP

Cyberfraud is abundantly *documented*. What is missing is a **mechanistic model of its propagation** that can be calibrated, analysed, and used for interventions.

FOUR CONTRIBUTIONS

01 Model

Five compartments, with an explicit victim to scammer pathway.

02 Theory

Well-posedness, $\mathcal{R}_0$, and global stability of the scam-free state.

03 Data

Bayesian calibration against 51 months of Canadian fraud reports.

04 Method

A finite difference scheme that is dynamically consistent.

Building the model

PART 2 OF 7

2

Five compartments

S	V	R	A_{s}	R_{s}
Susceptible	Victims	Temporarily aware	Active scammers	Removed scammers

THE BALANCE LAW

$$N(t) = S(t) + V(t) + R(t) + A_{\mathrm{s}}(t) + R_{\mathrm{s}}(t) \tag{1}$$

The population is *not* closed, so N is conserved, subject to certain condition.

Four modelling assumptions

Homogeneous susceptibility

Aggregate national dynamics; interaction enters through effective mass action, $\beta S A_s$.

An evolving scammer pool

A_s grows by external recruitment (δ) and shrinks by voluntary exit (μ) and enforcement (λ).

Temporary recovery

Prior victimisation confers *awareness*, not immunity. Awareness wanes at rate σ.

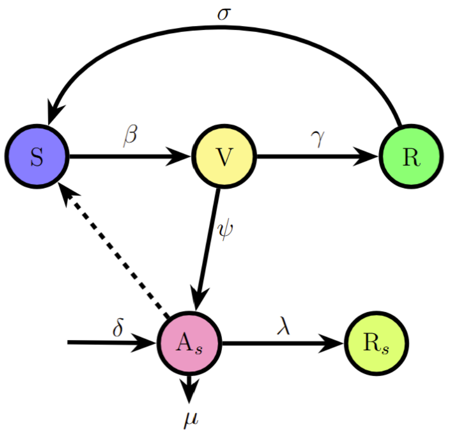
The victim to scammer pathway

Exploited individuals are recruited wittingly or not into facilitating fraud, at rate ψ.

WHY THE LAST ONE MATTERS

The fourth assumption is critical to this presentation. It turns a linear crime process into a **feedback loop**.

The flow of people through the system



Solid arrows: progression and recruitment.

Dashed arrow - transmission: contact between A_s and S that produces new victims.

THE LOOP TO WATCH

$$V \xrightarrow{\psi} A_s \dashrightarrow S \xrightarrow{\beta} V$$

Victims become scammers, who create victims. Cut this and the epidemic loses its engine.

The governing equations

$$
\begin{aligned}
\frac{dS}{dt} &= -\beta S A_s + \sigma R \\
\frac{dV}{dt} &= \beta S A_s - \gamma V - \psi V \\
\frac{dR}{dt} &= \gamma V - \sigma R \\
\frac{dA_s}{dt} &= \delta A_s - \mu A_s - \lambda A_s + \psi V \\
\frac{dR_s}{dt} &= \lambda A_s
\end{aligned} \tag{2}
$$

with $S(0), V(0), R(0), A_s(0), R_s(0) \geq 0$.

Amplifiers $\beta, \sigma, \psi, \delta$ — each pushes the system *towards* endemic fraud.

Suppressors γ, λ, μ — each drains victims or scammers out of circulation.

The parameters

AMPLIFIERS

β	Effective victimisation rate
σ	Rate at which awareness wanes
ψ	**Victim defection** into scammer roles
δ	Recruitment / growth of the scammer pool

SUPPRESSORS

γ	Rate at which victims become aware
μ	Rate of voluntary exit from scamming
λ	Rate of removal by law enforcement

A QUESTION TO HOLD ONTO

> These parameters are policy addressable. Which one leads to the most reduction in fraud per unit of effort?

Analysis and the threshold

PART 3 OF 7

3

Is the model legitimate?

Populations must stay non-negative and must not blow up

THEOREM 3.1: GLOBAL EXISTENCE

Since $0 \leq A_{\mathrm{s}} \leq N$, the balance law gives $\dot{N} \leq \delta N$, so

$$N(t) \;\leq\; N(0)\, e^{\delta t}. \qquad (3)$$

No solution blows up in finite time: the model is defined for all $t \geq 0$.

THEOREM 3.2: POSITIVITY

For non-negative initial data $(S(0), V(0), R(0), A_{\mathrm{s}}(0), R_{\mathrm{s}}(0)) \in \mathbb{R}^5_+$, all five state variables remain non-negative for every $t > 0$.

$N(0)e^{\delta t} \to \infty$, so Theorem 3.1 state **global existence**, not a bounded invariant region. Whether the orbit actually stays bounded is a separate question, and it has a sharp answer.

Boundedness: the sharp condition

Write $k = \mu + \lambda - \delta$ and $P_0 = S(0) + V(0) + R(0)$

THEOREM 3.3: IF $k > 0$, BOUNDED

Every orbit stays bounded:

$$P(t) \le P_0, \qquad A_s(t) \le \max\left\{A_s(0), \frac{\psi P_0}{k}\right\}, \qquad \int_0^\infty A_s\, ds \le \frac{A_s(0)+P_0}{k} \tag{4}$$

and hence $\sup_t N \le N(0) + (\delta - \mu)_+ \frac{A_s(0)+P_0}{k}$, with $V, R, A_s \to 0$.

THEOREM 3.4: IF $k \le 0$, UNBOUNDED

$\dot{A}_s = -kA_s + \psi V \ge 0$, so A_s never decreases and R_s, hence N, grows without bound, linearly when $k = 0$, at rate $e^{|k|t}$ when $k < 0$.

No bounded invariant region exists in this regime.

THE CONDITION FOR BOUNDEDNESS

$k > 0$ means $\delta < \mu + \lambda$: recruitment is outpaced by total exit.

What does a society free of cybercrime look like?

THE SCAM-FREE EQUILIBRIUM

$$\phi_0 = (S^*, V^*, R^*, A_s^*, R_s^*) = (N, 0, 0, 0, 0). \tag{5}$$

Everyone is susceptible; nobody is being scammed; nobody is scamming.

Susceptibility is not the problem, *activity* is.

THE CRITICAL QUESTION

Under what conditions does the system return to ϕ_0 **on its own**?

Anatomy of the scam reproduction number

By the next-generation matrix, $\mathcal{R}_0$ is the expected number of scammed individuals generated by one scammer introduced into a wholly susceptible population.

TRANSMISSION × DEFECTION

$$\mathcal{R}_0 = \frac{\beta\,\psi\,N}{(\gamma+\psi)(\mu+\lambda-\delta)}. \tag{6}$$

EXIT FROM VICTIMHOOD × NET EXIT FROM SCAMMING

Numerator

Fraud spreads only if scammers create victims (β) *and* victims become scammers (ψ).

Denominator

Fraud dies out if victims exit quickly (γ) and scammers leave faster than they are replaced.

The minus sign

δ enters the denominator **negatively**. Recruitment does not merely add, it *cancels* enforcement.

Stability, and the threshold at $\mathcal{R}_0 = 1$

IF $\mathcal{R}_0 < 1$

ϕ_0 is locally *and* globally asymptotically stable (via a Lyapunov function).

Cyber scams cannot sustain themselves and die out on their own.

IF $\mathcal{R}_0 > 1$

ϕ_0 is a saddle: an introduced scammer sets off an **outbreak**. Because the civilian pool only drains, the outbreak burns down to $S_\infty \leq S_c$ rather than settling on an endemic state.

Fraud persists for as long as susceptibles last.

THE POLICY READING OF A THRESHOLD

Law enforcement does **not** need to arrest every scammer. It needs enough *cumulative* pressure on λ, μ and δ to push $\mathcal{R}_0$ below one. Past the threshold, the rest of the decline is free.

Grounding the model in data

PART 4 OF 7

4

The evidence base

Canadian Anti-Fraud Centre, January 2021 – March 2025

328,649
complaint-level records

212,984
classified as *Victim*

51
monthly observations
January 2021 – March 2025

8,098
peak month; low of 2,364

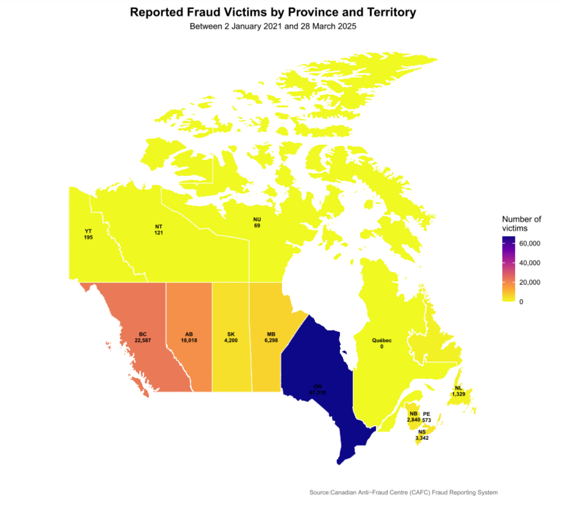
Target variable. The monthly victim count Y_m, matched against the model's $V(t_m)$.

> A national aggregate is exactly the right resolution for a mass-action model, and exactly the wrong one for claims about individuals.

Where the reports come from

Absolute counts track population centres; Ontario, Quebec, British Columbia, Alberta.

This is a sanity check rather than a modelling input: it tells us the signal is *national* in character, which is what licenses the aggregate treatment.



Bayesian calibration

Delayed Rejection Adaptive Metropolis (DRAM)

Sampler

MCMC with delayed rejection and an adaptive proposal covariance robust to the strong parameter correlations this model produces.

Objective

Fit the model predicted victim population $V(t_m; \Theta)$ to the observed monthly CAFC count Y_m.

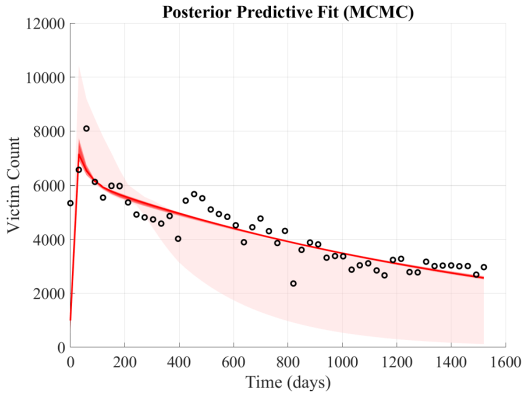
Budget

10,000 iterations, 50% discarded as burn-in.

UNCERTAINTY IS REPORTED, NOT HIDDEN

Posterior means, medians and **95% credible intervals** are computed for every transition rate so every conclusion that follows carries a stated confidence, not a point guess.

Posterior predictive fit



Open circles: observed monthly victim counts.

Solid line: posterior mean.

Shaded band: 95% credible region.

WHAT THE FIT CLAIMS

The model reproduces the **broad temporal pattern** of aggregate reported victimisation: the sharp early peak and the long decay.

Numerics that respect the model

PART 5 OF 7

5

Standard schemes can lie

THE PROBLEM

Classical finite difference scheme can produce **negative populations** or unrealistic solution unless step size h is severely constrained.

The remedy

A structure-preserving **non-standard finite difference** (NSFD) scheme, built on Mickens' rules.

The two ingredients

A non-traditional denominator function $\phi(h)$, and non-local approximation of the nonlinear terms.

THE PAYOFF

Positivity holds **unconditionally**, for *any* step $h > 0$; and the scheme is dynamically consistent.

The discrete scheme

Each transfer carries the same index in the donor and the recipient equation

$$\begin{aligned}
\frac{S_{k+1}-S_k}{\phi(h)} &= -\beta S_{k+1}A_{\mathrm{s}_k} + \sigma R_{k+1} \\
\frac{V_{k+1}-V_k}{\phi(h)} &= \beta S_{k+1}A_{\mathrm{s}_k} - \gamma V_{k+1} - \psi V_{k+1} \\
\frac{R_{k+1}-R_k}{\phi(h)} &= \gamma V_{k+1} - \sigma R_{k+1} \\
\frac{A_{\mathrm{s}_{k+1}}-A_{\mathrm{s}_k}}{\phi(h)} &= \delta A_{\mathrm{s}_k} - (\mu+\lambda)A_{\mathrm{s}_{k+1}} + \psi V_{k+1} \\
\frac{R_{\mathrm{s}_{k+1}}-R_{\mathrm{s}_k}}{\phi(h)} &= \lambda A_{\mathrm{s}_{k+1}}
\end{aligned} \tag{7}$$

where $\phi(h)$ is the non-standard denominator function defined as

$$\phi(h) = \frac{1-e^{-(\sigma+\mu+\gamma+\lambda+\psi)h}}{\sigma+\mu+\gamma+\lambda+\psi}.$$

POSITIVITY, FOR ANY $h>0$

$(S_{k+1}, V_{k+1}, R_{k+1})$ solve a 3×3 system whose matrix is a non-singular M-matrix, so its inverse is non-negative; $A_{\mathrm{s}_{k+1}}, R_{\mathrm{s}_{k+1}}$ then follow explicitly. All five stay ≥ 0, **whatever** h.

AND THE CONSERVATION LAW HOLDS

$$P_{k+1}-P_k = -\phi(h)\,\psi V_{k+1} \;\leq\; 0 \tag{8}$$

holds *exactly*, as does the discrete form of $\dot{N} = (\delta-\mu)A_{\mathrm{s}}$.

Which parameter moves the system?

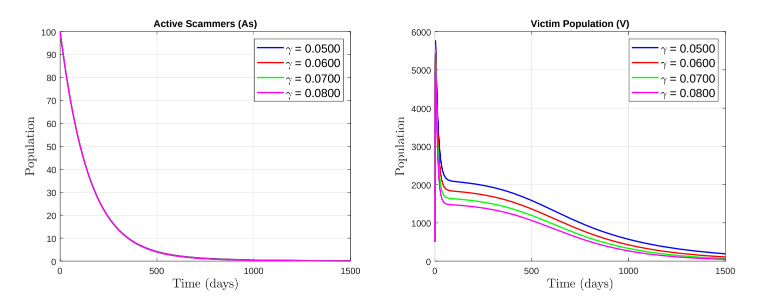
PART 6 OF 7

Victim recovery γ: helps victims, not the epidemic

AMPLIFY β σ ψ δ γ λ μ SUPPRESS

Raising γ mean faster transition of victims into an aware state steadily reduces the victim population.

But look at the left-hand panel: the **active scammer curves lie on top of one another**.



SURPRISE FINDING

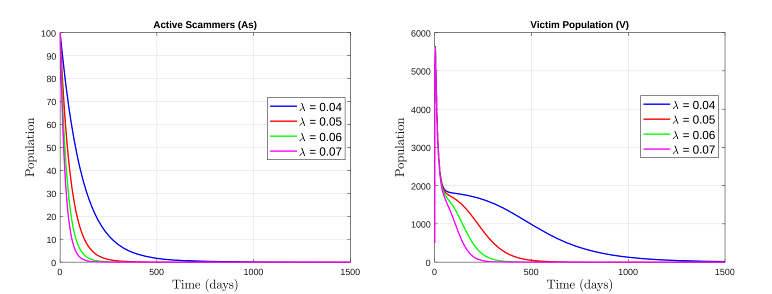
Awareness campaigns have a **negligible** effect on the active scammer population. Scammers simply pivot to the remaining susceptible pool.

Enforcement λ: it works, but it is expensive

AMPLIFY β σ ψ δ γ λ μ SUPPRESS

Higher arrest rates crash the scammer population, and the victim population follows with a lag.

This is the conventional cyber defence policy already in use.



BASELINE

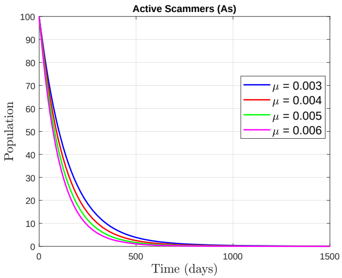
Enforcement is genuinely effective. The question is whether anything gives a larger return per unit of effort, the next slide says yes.

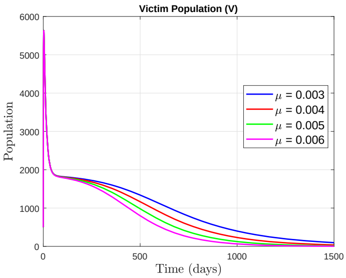
Voluntary exit μ: the cheapest lever in the system

AMPLIFY β σ ψ δ | γ λ μ SUPPRESS

Scammers who quit of their own accord have a **significantly greater systemic impact per unit** than scammers removed by arrest.

The network is highly fragile to internal turnover.





READ THIS AS AN ECONOMIC CLAIM

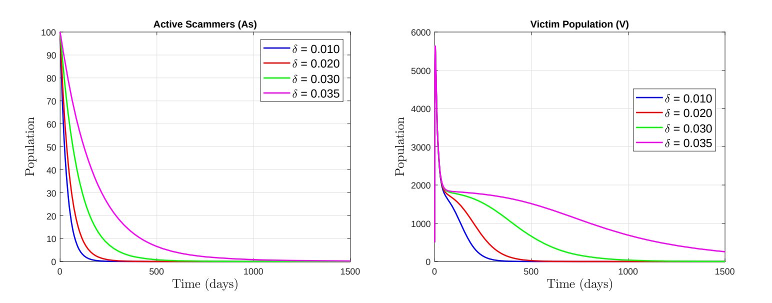
Making scamming an *unappealing career* through socioeconomic alternatives and deterrent policy competes with, and can outperform, arresting people.

Recruitment δ: the primary driver of longevity

AMPLIFY β σ ψ δ γ λ μ SUPPRESS

The ability to recruit new members is the **primary driver of scam longevity**.

Raising δ stretches the collapse of the scammer population from a matter of *days* to a matter of *years*.



WHY THIS DOMINATES

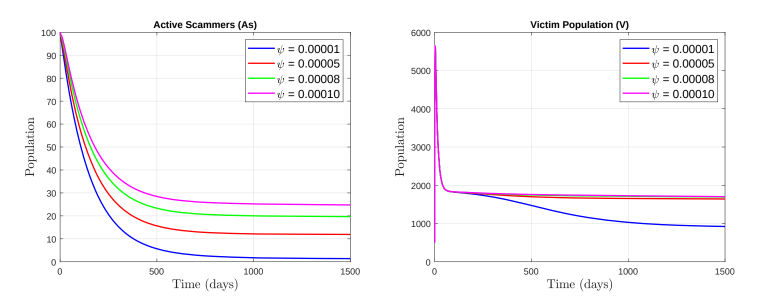
Recall that δ enters $\mathcal{R}_0$ as $(\mu + \lambda - \delta)$. Recruitment does not merely add scammers, it directly **cancels** enforcement effort.

Defection ψ: the sole source of persistence

AMPLIFY β σ ψ δ | γ λ μ SUPPRESS

ψ is the rate at which victims move into scamming roles.

Where δ *scales* the operation, ψ makes it **self-regenerating**: the curves settle on distinct non-zero plateaus.



THE STRUCTURAL RESULT

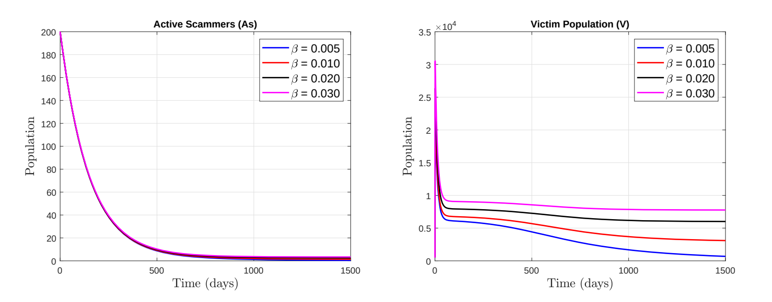
ψ is mathematically the **sole driver of long-term endemicity**. As $\psi \to 0$ the numerator of $\mathcal{R}_0$ vanishes and the network loses its regenerative mechanism.

Susceptibility β: it sets the toll, not the outcome

AMPLIFY β σ ψ δ γ λ μ SUPPRESS

Higher β drives up the steady state *victim* population, as expected.

But it has a **negligible** effect on the long run fate of the active scammer population.



THE COUNTER-INTUITIVE PART

Scammers are constrained far more by their **own lifecycle** such as recruitment, attrition, enforcement than by the supply of available targets.

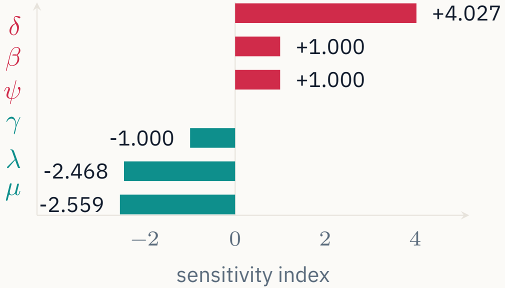
The scoreboard

Effect of increasing each rate on the two populations that matter

RATE	SCAMMERS A_s	VICTIMS V	VERDICT
β susceptibility	negligible	raises steady state	sets the toll
γ awareness	negligible	lowers steadily	humanitarian, not systemic
λ arrests	strong crash	strong, lagged	effective, costly
μ voluntary exit	**strongest per unit**	strong	best return on effort
δ recruitment	**sets collapse time**	prolongs	primary driver
ψ defection	sets the plateau	sets the plateau	sole route to endemicity

Local sensitivity of $\mathcal{R}_0$

Percentage change in $\mathcal{R}_0$ per 1% change in each parameter



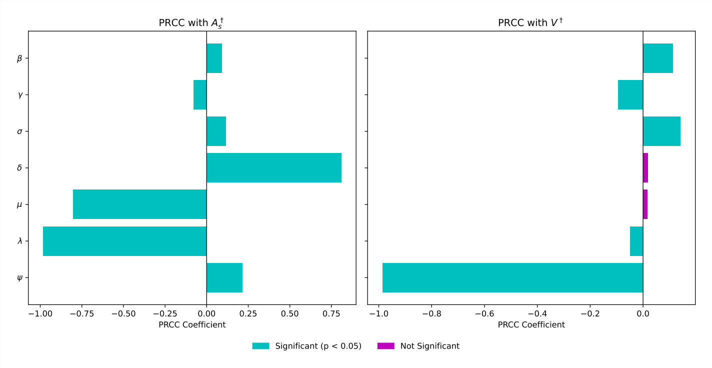
THE HEADLINE NUMBER

A **1% increase in recruitment** δ raises $\mathcal{R}_0$ by **4.03%**, four times the parameter of susceptibility, and more than either enforcement parameter can undo.

β and ψ are almost exactly unit elastic; the wo removal rates sit near -2.5.

Global sensitivity: PRCC

Long-run, cumulative, monotonic relationships across the parameter space



Accumulated scammers $A_s^\dagger$

Suppressed by arrests ($\lambda = -0.98$) and dropout ($\mu = -0.80$).

Accumulated victims $V^\dagger$

Dominated by victim defection ψ — the largest coefficient in the panel.

What follows for policy

PART 7 OF 7

7

Three things to take away

1. **Target the lifecycle, not the target.**
   Proliferation is driven by scammer recruitment and attrition rather than by victim susceptibility. δ carries four times the elasticity of β.

2. **Break the feedback loop.**
   Preventing victims from becoming mules or scammers, even at very low rates is what removes endemicity. ψ is the only structural route to a self-sustaining fraud economy.

3. **Encourage attrition.**
   Making scamming an unappealing career (raising μ) is a powerful *internal* lever, and per unit of effort it outperforms external arrest.

Policy recommendations

SHIFT FROM REACTIVE TO PROACTIVE

Conventional cyber defence prioritises reactive policing. This analysis says the binding constraint is the set of **internal feedback loops** that regenerate the scammer population.

Disrupt the pipelines

Systematically flag and dismantle digital recruitment channels.

Reduces δ; the highest elasticity parameter in the model.

Prevent defection

Rapid post scam counseling and financial support, so victims are not pushed into coercive money mule roles.

Reduces ψ; the sole driver.

Coordinate

Law enforcement, financial institutions and hosting platforms each control different rates.

No single actor controls enough of $\mathcal{R}_0$ alone.

Limits of the present model

01 Close the population

Let quitters return to society; add $+\mu A_s$ to $\dot{S}$ and draw recruits from S rather than from outside.

Consequence: an exact conservation law, $\dot{N} \equiv 0$.

02 Add demography

A recruitment Λ into S and a per-capita exit rate ν from every compartment.

03 Allow recidivism

Removed scammers re-enter: $\dot{R}_s = \lambda A_s - \rho R_s$, with $+\rho R_s$ added to $\dot{A}_s$.

Consequence: an endemic state in a closed population, and a new policy dial, ρ measures the quality of rehabilitation.

BEYOND THE STRUCTURE

Then the empirical extensions: provincial metapopulation structure, time-varying δ and ψ tied to macroeconomic covariates, optimal control under an enforcement budget, and a stochastic version to quantify extinction probability near $\mathcal{R}_0 = 1$.

Thank you

Cut the loop, not just the losses.

Yusuf Olatunji Tijani • Wits & Rhodes

All models are wrong, but some are useful.

Questions welcome

Get in touch

- yusuf.tijani@wits.ac.za
- olodyusuf@gmail.com

Yusuf Olatunji Tijani

School of Computer Science and Applied Mathematics, University of the Witwatersrand

Department of Mathematics, Rhodes University