Scams are now a national security issue

26 Jun 2024 | **Paul Curwell** and **Nicholas McTaggart**

Scams are no longer just a consumer fraud problem. While responsibility for scams in Australia primarily resides with regulators, sophisticated scams have become issues of counter-terrorism (CT) and transnational serious and organised crime (TSOC) that are under-recognised by national security and law enforcement communities.

More must be done to counter scammers' use of artificial-intelligence technology, which is increasing the volume and sophistication of their crimes. National security and law enforcement communities need to bolster their targeted intelligence collection and coordinated intervention, and they must be supported by robust asset tracing and greater punitive measures.

It seems that everyday we hear of someone who has fallen victim to a scam, a deeply shameful and life-changing experience for many. Scams rely on social engineering and behavioural manipulation to convince the target to act against his or her own interests. Victims are identified and contacted in large numbers through social media and email, with banks used as a vehicle to exfiltrate funds.

In 2023 Australians lost $2.7 billion to scams, with global losses totalling nearly US$1.026 trillion, not to mention unquantifiable social and personal impacts (including suicides) with downstream costs to Australia's health budget. In the past year, the number of scams reported in Australia increased by 18.5 percent to more than 600,000. Technology helps propagate scams, and losses are likely to skyrocket further with the advent of generative AI, which will test societal resilience, cybersecurity measures and consumer confidence in Australia's financial and identity systems.

While some scams are still conducted locally by opportunistic criminals, many perpetrators are now making fortunes running industrial-scale scam operations internationally. The magnitude of these operations is stunning, and their impact not constrained to fraud victims. A police raid in the Philippines in March this year against a TSOC-operated, 25-hectare, 36-building complex rescued nearly 900 people forced to work in scams. They came from seven nationalities.

In 2023, Reuters identified over 200,000 employees of TSOC-run scam operations across Southeast Asia, including job seekers who had foreign university education and who had been lured under false pretences. Some were also victims of human trafficking and slavery. In many cases, workers are exposed to extreme violence and law enforcement officials are bribed or intimidated to turn a blind eye.

Asia and Africa are hubs for scams and TSOC, but such large-scale operations can also be found in Australia. In February this year, Queensland Police uncovered an operation on the Gold Coast that had scammed victims of millions of dollars.

Scams are now being used by terrorist groups and countries as highly effective financing vehicles. In 2022, *The Times* revealed how ISIS was funding insurgencies across Asia by scamming South Africans through fake Tinder profiles. And, this year, financial news outlet CE Noticias Financieras dissected the relationship between Hezbollah and Brazillian TSOC group PCC, outlining how PCC used scams to finance its activities and how Hezbollah associates helped PCC buy and smuggle weapons.

The low-risk, high-reward nature of scams means that more pervasive, sophisticated adversaries have displaced opportunistic low-level criminals—and are largely remaining off the radar. Money mule schemes divert funds from victim to criminal-controlled accounts, often using cryptocurrency to evade anti-money laundering and sanctions controls. In 2023, Canada's financial intelligence agency, Fintrac, reported that Russian parties had received a disproportionate share of all cryptocurrency-enabled crime, including online frauds, raising the prospect of orchestrated sanctions evasion.

While there is no evidence in the public domain to support this, there is likely a connection between scams and large-scale data or identity breaches. Persistent data breaches provide information that can be used in advanced scam campaigns to inform targeting and customise victim selection. Scammers can use biographical information as well as data on social interactions and relationships to trick potential victims. As social media becomes increasingly prolific and its data easier to harvest at scale via AI, we may see even greater personalisation of scam communications. Already, data breaches help perpetrators of some scams initiate friendships with victims before luring them into trading money on a fake platform.

Against this threat landscape, anti-scam responses by governments across the world are inadequate. They are skewed towards costly taxpayer-funded band-aid solutions that treat the symptoms rather than cure the disease. The sophisticated, highly adaptive criminal and terrorist networks operating lucrative global scams cannot be disrupted through reactive programs and internal controls alone.

Scam networks now require attribution and carefully targeted disruption, ideally using a combination of cyber, financial, enforcement and international-development capacity. As the US Department of Defense said in 2016, 'defeating transnational threats requires the synchronization, coordination, and integration of all the instruments of national power in cooperation with regional and multinational partners'.

The global scams epidemic is at a tipping point. Law enforcement and national security communities need more resources for targeted intelligence collection and coordinated intervention against scam channels, scam infrastructure and illicit businesses. This should be supported by robust tracing and forfeiture of financial assets where criminal funds interface with the legitimate global economy. This would reduce criminal incentives and allow seized assets to be diverted to pay for prevention measures and community awareness initiatives.

These changes should happen now, as the latest versions of AI will have a dramatic impact on the threat landscape and likely reverse recent gains made through improved technology and awareness campaigns. Make no mistake, this is a battle which can be won only by altering the status quo back in our favour.

AUTHOR

Paul Curwell is a principal in the fraud and intelligence practice at Deloitte, a lecturer in fraud and financial crime at the Australian Graduate School of Policing and Security, Charles Sturt University, and co-author of Terrorist Diversion (Routledge, 2021). **Nicholas McTaggart** is the founder of The Murinbin Group, a specialist financial crime consultancy, and the former national coordinator of the Criminal Asset Confiscation Taskforce at the Australian Federal Police. Image: US Federal Bureau of Investigation.

TAGS

Australia | artificial intelligence | organised crime

SHARE

Error: Twitter was not able to process that request

Subscribe to *The Strategist*

Full Name

Email

DAILY | WEEKLY

CRITICAL TECHNOLOGY TRACKER

Visit ASPI's homepage

RELATED POSTS

Australia needs a better strategy for fighting organised crime

Malicious AI arrives on the dark web

Our drug policies aren't working. The evidence is in wastewater

Transnational serious and organised crime: we need a white paper

Pacific islands are no longer free of organised crime