Scam centres in the Blue Pacific: a security threat we cannot ignore

Arrests in a Palau scam centre
Photo Credit: Palau National Security Coordination Office

by Ayanna Ramarui

29 June 2026

A real and pressing security concern is emerging in the Pacific. There has been an increase in online scamming, a complex and evolving threat that is relatively new to the region.

This shift seems to be part of the expansion of transnational crimes into vulnerable small island states.

Online scam centres are large-scale and highly organised criminal operations that often rely on forced labour to carry out global cyber fraud. Victims of human trafficking are forced to conduct "pig butchering" — where scammers build trust through fake relationships before tricking victims into investing in fraudulent schemes, often cryptocurrency schemes — and romance scams while being held inside heavily guarded compounds. Individuals are often lured with fake job offers, made to surrender their passports upon arrival, and subjected to threats, violence and other forms of coercion.

These operations are commonly found in Southeast Asia, in countries such as Cambodia, Myanmar and Laos. Operators behind these scam centres typically use social media platforms, dating applications and messaging services to target and manipulate victims around the world.

One of the most notorious cyber scam hubs, KK Park in Myanmar, was raided in 2025. The compound was associated with online fraud, money laundering and human trafficking. During the raid, more than 2,000 workers were released and 30 Starlink satellite terminals were confiscated. Reports indicate that thousands of people had been lured to the compound with promises of well-paid employment but were instead forced to run elaborate scams, stealing billions of dollars from victims.

Operations that were previously concentrated in Southeast Asian countries are now attempting to establish themselves in Pacific Island countries. Palau, Tonga, Fiji, Vanuatu, Timor-Leste and Papua New Guinea have encountered elements of this evolving threat. According to the Organized Crime and Corruption Reporting Project (OCCRP), a scam centre uncovered in Palau had connections to Chinese criminal syndicates. Individuals involved operated from abandoned or enclosed buildings, having entered Palau as tourists before applying for work permits.

Palau faces significant challenges in responding to online scams. With no cybercrime laws or regulations in place and limited technical resources and

investigative capacity, it is difficult for law enforcement to effectively detect, prosecute and dismantle these networks. Many people working within these operations are believed to be victims of human trafficking, further complicating enforcement efforts.

In a report on the Pacific's evolving threat landscape, the United Nations Office on Drugs and Crime highlights the growing risks posed by transnational organised crime in the region. Drug trafficking, money laundering and the proliferation of cyber-enabled fraud — including large-scale scam centres where workers are trafficked and abused — are emerging and interconnected threats.

In 2025, a raid was carried out in the Oecusse region of Timor-Leste, where a "digital centre" was discovered. The centre was making use of Starlink satellite devices and multiple SIM cards to operate large-scale online scams. The fact that this kind of activity was uncovered in Timor-Leste suggests that scammers are spreading out across the region. Such operations are no longer isolated incidents, but part of a broader shift.

With limited expertise, legislative gaps and constrained enforcement capacity, Pacific Island states face significant obstacles in addressing this threat. As transnational criminal networks recognise the vulnerabilities of small developing island states, the Pacific is increasingly becoming an attractive target for exploitation.

Regional initiatives such as Cyber Safety Pasifika have played a significant role in strengthening cyber awareness and investigation capabilities across the Pacific. But these programs appear to focus mainly on cyber awareness and general investigative training rather than specifically addressing the emerging threat of organised online scam centres.

Amid growing evidence that such scam centres are beginning to relocate to the Pacific, a more targeted regional response is needed. Some recommendations we can consider include:

Strengthening national legislation: Pacific Island countries should review and strengthen their existing cybercrime legislation to specifically address cyber-enabled fraud operations. Countries that do not yet have the necessary legal frameworks in place should seek assistance from others in the region that already have such legislation and learn from their experiences and best practices.

Integrating a scam centre focus into regional cyber programs: Regional initiatives such as Cyber Safety Pasifika could include a dedicated focus on the detection, prevention and disruption of organised scam centres. This could include specialised

training on identifying scam centre indicators, cryptocurrency tracing, digital financial investigations and intelligence-led policing approaches.

Enhancing regional intelligence sharing: Through mechanisms such as the Pacific Islands Chiefs of Police network, Pacific countries should strengthen intelligence sharing and joint investigations related to transnational cyber fraud syndicates. Establishing early warning systems and coordinated regional responses will help prevent these criminal networks from exploiting vulnerabilities within smaller jurisdictions.

Given the vulnerabilities of small island states, a collective and proactive regional response is essential.

This is a lightly edited version of an article first published on the Pacific Wayfinder blog, a platform of the Pacific Security College at the Australian National University.

Author/s:

Ayanna Ramarui
Ayanna Ramarui is a policy analyst within Palau's National Security Coordination Office, where she supports national initiatives related to security and foreign affairs.

Link:
https://devpolicy.org/scam-centres-in-the-blue-pacific-a-security-threat-we-cannot-ignore-20260629/