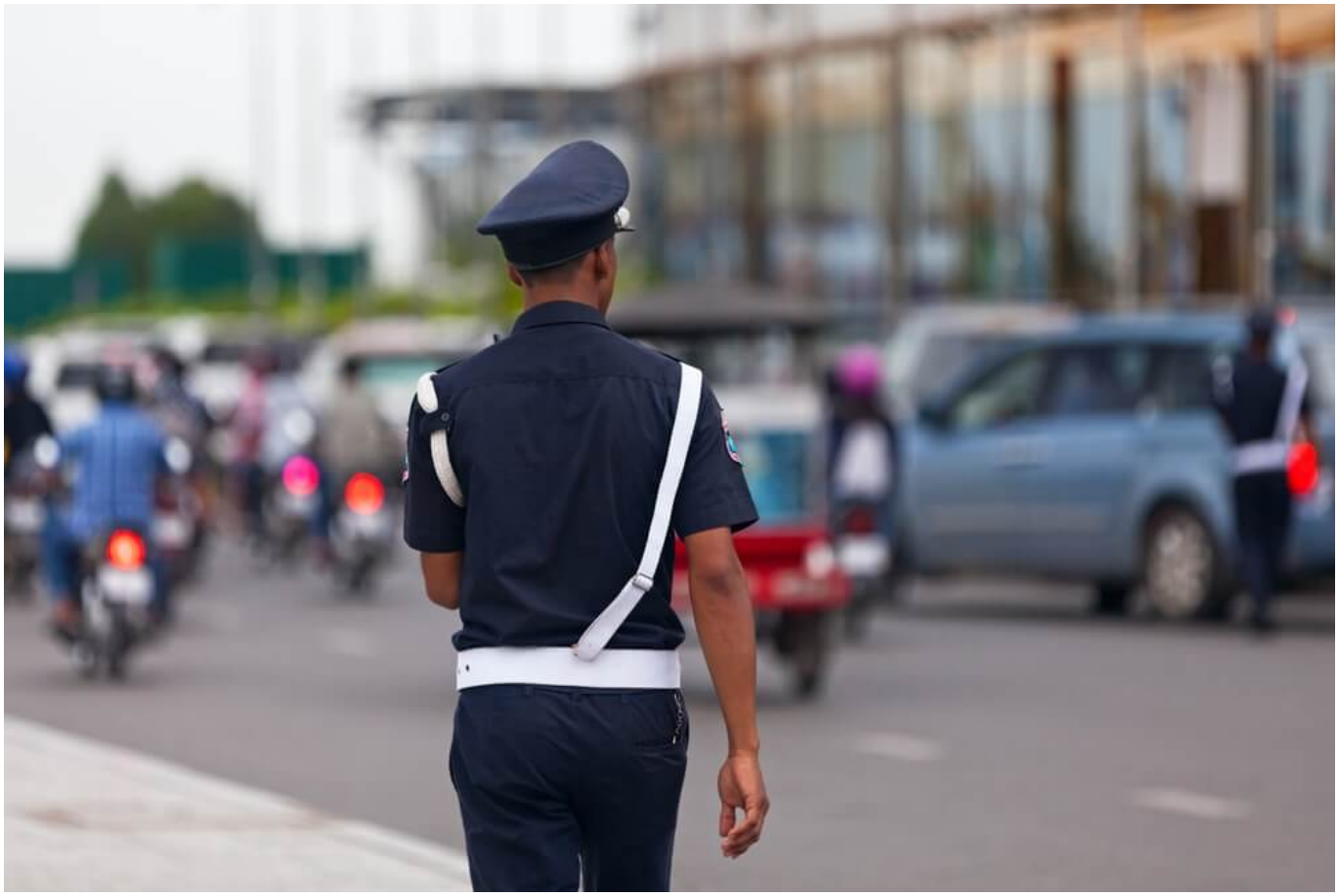
Tomorrow's Affairs
Analysis of today
Assessment of tomorrow

By: Tomorrow's Affairs Staff

Crime as infrastructure – the case of Cambodia



Cambodia has become the centre of a new type of organised crime. In a country that until recently was known for its textile facilities and tourist zones, an online fraud industry has emerged, operating as a legal business.

The industry has a precisely organised structure, global financial flows, and a forced workforce. There is no improvisation: the camps, employing tens of thousands of people, operate as closed systems that measure, monitor, and control everything.

In these camps, classic frauds are not committed from the shadows; instead, a digital illusion of trust is created.

Operators contact victims worldwide—usually through social networks, dating apps, or investment platforms—by posing as brokers, cryptocurrency traders, or individuals who offer to partner in "safe investments."

Everything is carefully planned, from fake profiles and fake conversations to websites that look like real banks and even video calls with generated faces and voices.

Once the victim is drawn in and transfers money, communication is abruptly cut off and all traces vanish. Behind each such contact is a team of people confined in a camp, working in shifts, with set targets and supervisors who monitor performance, as in a corporation.

The economy of coercion

In October, South Korea announced that it had deported 64 of its nationals from Cambodia for involvement in digital fraud. More than fifty were detained, some as victims, others as perpetrators.

This is the first systematic attempt by a state to recognise and distinguish the complex roles in the new economy of coercion.

Until now, these camps have been described as "places where people are cheated over the Internet." It is now clear that this is an industrial model combining elements of slavery, organised crime, and the legitimate labour market.

> What starts as online fraud targeting victims turns into fraud against the workers themselves, who are exploited as tools in the chain of coercion

Recruitment is straightforward. Well-paid technology jobs are advertised on social media and job sites. Upon arrival, workers' passports are confiscated, rules and quotas are imposed, and failure to meet targets results in fines or new debt.

Each operation is backed by a network of managers, IT experts, local intermediaries, and financial operators who control the flow of money.

What starts as online fraud targeting victims ultimately turns into fraud against the workers themselves, who are exploited as tools in the chain of coercion.

An example of a global trend

Cambodia is not an exception but an example of a global trend. Maps from UNODC and Interpol indicate the identification of similar centres in Myanmar, Laos, and Thailand. Some are moving further afield – to East Timor and parts of Africa.

The reason is not only weak oversight but also the ability of these networks to exploit legal channels. They register as "tech companies", pay taxes, and open bank accounts.

This is what international institutions still do not fully understand: crime no longer hides; it has integrated into structures that states and markets consider legitimate.

> Traditional legal frameworks no longer recognise the nuances of coercion in a digital environment

South Korea's response demonstrates a new model of state action. In addition to police operations and diplomatic pressure, a coordination mechanism has been established between the prosecutor's office, ministries, and the financial sector.

Repatriation is no longer merely a humanitarian measure; it has become an instrument of investigation. Each return from the camps raises the question: was the individual an accomplice, mediator, or detainee?

Such differentiation is crucial, as traditional legal frameworks no longer recognise the nuances of coercion in a digital environment. In this model, the victim and perpetrator are often the same person, distinguished only by when they lost the ability to choose.

When capital moves faster than regulation

The next phase is the transition of the system to automation. Camps already employ generative tools that enable a single operator to conduct dozens of conversations with victims simultaneously.

Voices and images are artificial, scenarios are predefined, and responses are practised to the point of automaticity.

This reduces the need for mass labour but increases the average damage per person deceived. Crime no longer depends on physical space but on software infrastructure, making it more resilient and portable.

> When capital moves faster than regulation, the only way to maintain order is for regulation to outpace the movement of money

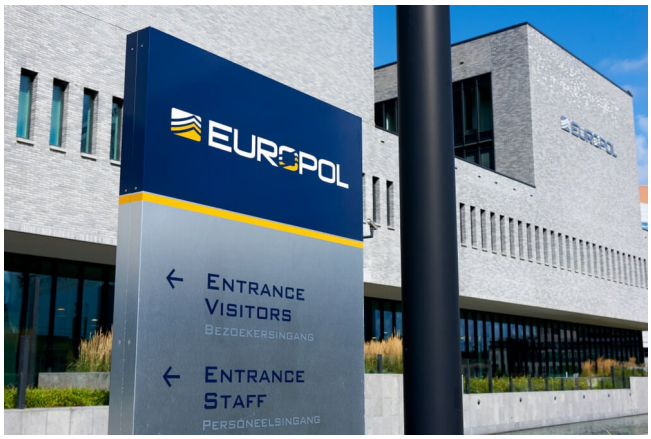
The strongest resistance comes from the financial sector, where, for the first time, a model for recognising behavioural patterns—rather than merely blocking known addresses— is being implemented.

Banks and payment processors analyse flows that indicate unusual activity: short-term accounts, mass micro-transactions, repeated refunds, and links to the same digital traces.

The issue is not technological but one of political will to identify and sever the legal channels that sustain illegal networks. When capital moves faster than regulation, the only way to maintain order is for regulation to outpace the movement of money.

The same system, the same banks, the same digital tools

In this context, Cambodia is not only a site of crime but also a reflection of the global system. While Europe and the United Kingdom address data protection and privacy concerns, financial flows originating from Asian camps pass through the same channels used by legitimate companies.



While Europe and the UK address data protection and privacy concerns, financial flows originating from Asian camps pass through the same channels used by legitimate companies

Crime does not operate in a parallel world; it uses the same system, the same banks, and the same digital tools. The only difference is in purpose.

If states do not bring police, banks, and technology platforms into a unified response system, the camps will simply keep moving.

If they do, there's a significant risk that their economy will collapse – not due to arrests, but due to the loss of profits. This approach introduces a significant shift: the end of crime is not the capture of perpetrators, but rather its unprofitability.

Today, Cambodia serves as a laboratory for testing the limits of state power. It demonstrates what happens when crime moves from the shadows into the market structure, when work becomes an instrument of coercion, and fraud becomes a standardised product.

What we see there is not an Asian problem but a global model that is spreading to places where the economy and the legal system do not interact quickly enough. Once that model enters legal channels, borders cease to be real.