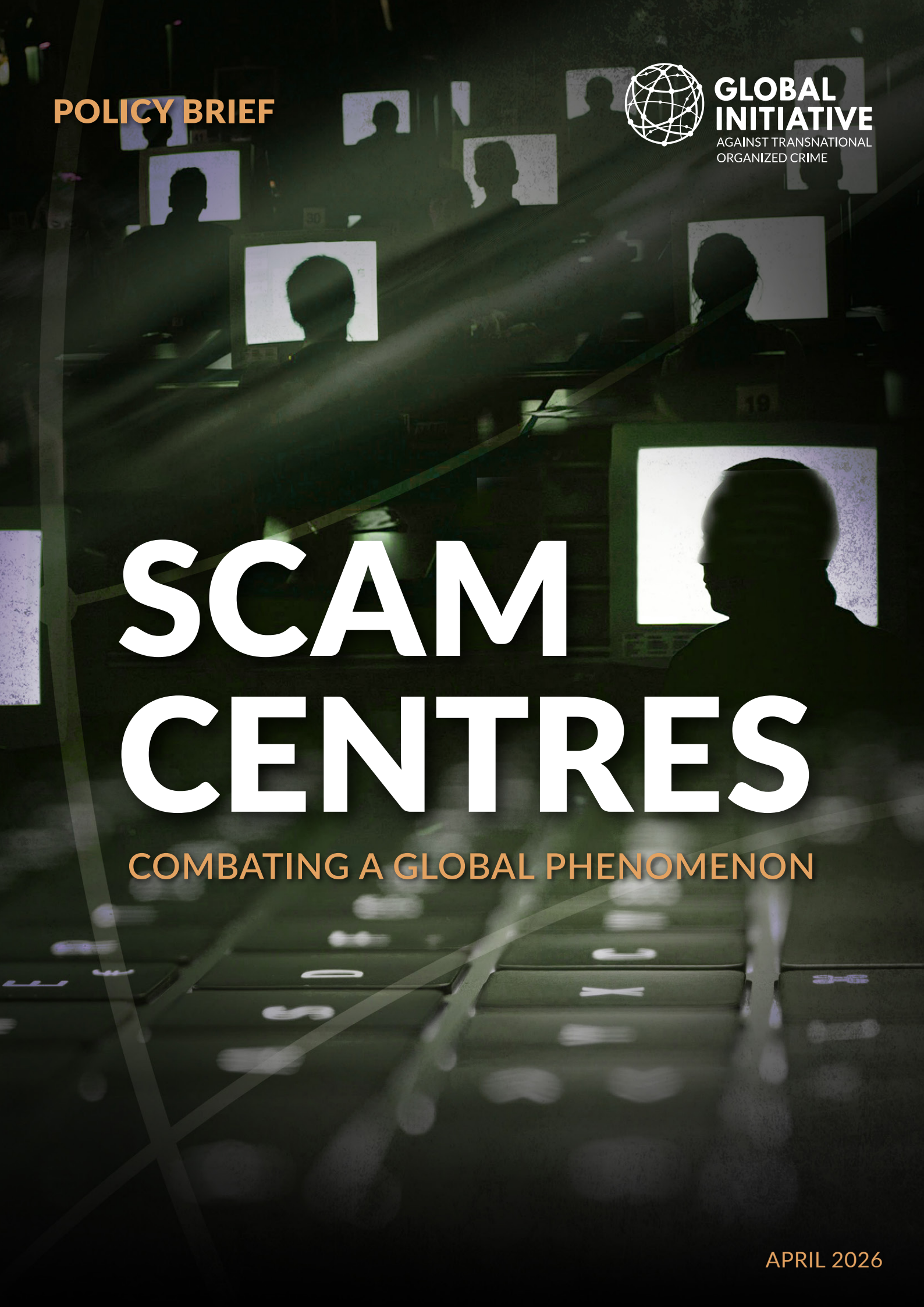


POLICY BRIEF

GLOBAL INITIATIVE
AGAINST TRANSNATIONAL ORGANIZED CRIME

SCAM CENTRES

COMBATING A GLOBAL PHENOMENON

APRIL 2026

Cover: © *David Trood/DigitalVision via Getty Images, Unsplash*

Please direct inquiries to:
The Global Initiative Against Transnational Organized Crime
Avenue de France 23
Geneva, CH-1202
Switzerland
www.globalinitiative.net

CONTENTS

SUMMARY

This policy brief synthesises the findings of the Global Initiative Against Transnational Organized Crime (GI-TOC)'s investigation into scam centres in Eurasia and globally.[1] It aims to provide a concise, policy-orientated overview of the nature and scope of the issue of scam centres, and provide focused recommendations.

Key points

- The scam centre has emerged in recent decades as one of the most sophisticated, lucrative and pervasive forms of organized crime in the world today. According to the Global Scam Alliance, scammers stole more than US$1 trillion in 2024 – representing almost 1% of world GDP.[2] Given the present state of play, the damage inflicted and the potential path of travel, it is vital that responses become more holistic, strategic and coordinated, grounded in a thorough understanding of how the scam centre ecosystem functions. Otherwise, the situation will only worsen.
- The pace of change has been rapid. Information and communications technology has fuelled an expansion both in the reach and sophistication of scammers, enabling them to target victims anywhere in the world. Social engineering – the psychological manipulation of victims to persuade them to hand over financial details and/or money – is at the heart of scam centres. By constructing such relationships, for romance, impersonation and investor scams, criminals can steal large sums of money, sometimes running into millions of dollars or depleting entire life savings.
- Scammers are the tip of a criminal iceberg. A whole host of actors and tools are involved in creating the perfect scam, including transnational criminal networks, digital marketeers, decentralized finance, crypto exchanges, leaked databases, AI technology and money mules, to name but a few. The barriers to entry are low: scams require little in the way of enabling infrastructure, and what is required is easily obtained. Crime-as-a-service, where threat actors sell packaged tools or services used to deploy attacks, makes it easy for would-be scammers to buy in the components needed, from scripts to databases, customer-relationship management (CRM) software and money laundering services.
- Scam centres are present around the world. They manifest in various shapes and sizes, from individuals working in prison cells and apartments to large-scale outfits based in centrally located office spaces or compounds. They may operate under the guise of legitimate businesses or may in fact be legitimate businesses moonlighting as scam centres, blurring the distinction between legal and illegal. In many places, scam centres are located or run their operations as part of online service companies, offshore gambling operations, special economic zones or legitimate call centres that provide customer support.

- Scam centres are locally based, but they make use of global-level force multipliers. GI-TOC research has identified six: the ability of scam centres to network, technology and crime-as-a service, money laundering infrastructure, political protection, people and geopolitics. These six ingredients help to explain why scam centres have become such a potent form of organized crime that has spread so widely – and why they are so challenging to address.
- Looking ahead, increased law enforcement attention on certain hubs of activity may see scam centres displaced to new countries, especially those where they can work with corrupt actors who will offer protection. They may also become more diffuse, shifting from large-scale models to smaller, more networked operations, reducing their public profile. And as the world becomes more deglobalized, scam centres will increasingly exploit rifts in law enforcement cooperation and capitalize on new narratives.

Recommendations

Scam centres around the world have come under increasing law enforcement pressure in recent years, with some impressive results. Billions of dollars have been seized from scammers and major networks dismantled.

But such is the ease of entering the scamming economy – and the riches on offer – that new participants will not be in short supply. It is therefore critical to address the enabling environment in which scam centres flourish, and to treat them with the same degree of focus as we do other major forms of organized crime.

1. **Harmonize tools of leverage, at home and abroad.** Scams are a global problem and must be tackled by international partners working in tandem. Improve coordination among law enforcement agencies: pool resources, knowledge and leads, and share lessons learned. Use diplomatic and economic tools to put pressure on countries where strong political protection allows scam centres to operate, and improve cooperation with countries that may be vulnerable to displaced scam centres. Revise domestic legislation to increase accountability for social media, financial services and other forms of technology used by scammers.
2. **Improve international cooperation between geopolitical rivals.** Between countries with strong political disagreements, explore case-by-case basis cooperation on scam centres. Without such action, scam centres will continue to exploit geopolitical divisions and operate with impunity.
3. **New thinking for new challenges.** To address the threat of AI, new tools and strategies are required. Broad coalitions involving technology firms, law enforcement, government and civil society could help. A combination of safeguards, digital and financial literacy campaigns, and defensive AI tools will also be necessary.
4. **Reintegrate former scammers into the mainstream economy to prevent proliferation.** Establish employment pathways for trafficked scammers to prevent them from returning to fraudulent activities once they are back home. It may be worth considering a reassessment of criminal liability for actions performed under duress to prevent trafficked scammers from being blocked from the legal job market. Scammers who have not been trafficked also pose a skills proliferation risk. Ultimately, keeping track of who returns and what skills and profile they have is essential to determining the appropriate response, ranging from rehabilitation to monitoring and potentially indictment – another powerful argument for law enforcement cooperation.

THE SCAM CENTRE ECOSYSTEM

While the term 'scam centre' may conjure images of the vast compounds in South East Asia, in reality the organizational model is highly flexible, appearing in different shapes and sizes across the world. Prison cells, apartments, houses, office buildings and compounds can all host scam centres – and each format has its own advantages and disadvantages, as far as the scammers are concerned. The physical footprint of a scam centre also shapes its business model to some degree, often in unexpected ways.

Scam centres in prisons, for example, are often able to work without fear of official sanction, due to the close involvement of corrupt officials in enabling or even directing their work. However, the physical limitations of the prison context means that complex setups are generally not possible. Scammers must make do with phone calls and an internet connection, although these can still be highly effective tools.

Apartments and houses in residential areas offer a discreet base for scammers, allowing them to hide their activities behind closed doors. Some upscale residences come with private security, adding an extra layer of protection. Villas in rural areas are also sometimes used by scammers, keeping them even further away from prying eyes. Hotels are a quick-start option, requiring a minimum of preparation, and sometimes host years-long operations. Ease of relocation is a benefit for all these options: should there be signs of unwanted attention, scammers can pack up and leave without having to dismantle a large-scale operation.

The modest appearance of such operations can be misleading. In South Africa, for instance, Nigerian scammers may work in apartments or houses in small groups – up to about half a dozen – but they are often linked to broader networks, in effect representing a cell of a dispersed scam centre. This setup provides all the benefits of a large organization – shared resources, knowledge, expertise, managerial direction and economies of scale – without the public profile that would result from gathering all these elements in one place.

Large-scale offices closely resemble their legal call centre counterparts, with departments handling various aspects of the business, from IT and finance to HR and security. Those based in office towers are often difficult to spot from the outside. The scam compounds of South East Asia are the acme of this model: self-contained buildings that control the lives of their workforce and function almost as autonomous islands. Some of these operate in areas of grey governance in border zones or places

controlled by powerful political elites and military figures, while others are based in big cities and even capitals – there to see in plain sight. Due to their size and conspicuous nature, office-based scam centres and compounds are dependent on high-level political protection.

Social engineering: the personal connection

Scammers tend to draw upon a common toolbox of techniques (see box below), many of which involve social engineering. Unlike spamming, where a scammer sends out a huge volume of messages in the hope that a victim will respond, social engineering places the creation of a relationship between the scammer and the victim at the heart of the scam.

This can be achieved by using information harvested from social media and the dark web to create a list of promising potential victims, or to provide the scammer with information that establishes their credibility when contacting the victim for the first time. If a scammer pretending to be from a bank, for instance, already knows the victim's account details, place of residence and date of birth, and requires only a few details 'to be confirmed', the victim may be more inclined to provide the last crucial pieces of information needed to access their account.

Social engineering can also take place after the initial deception has begun, as is the case with romance fraud. In this case, the scammer attempts to establish a connection with the victim, building trust and intimacy, sometimes over extended periods of time, until the point that a request for money can be made. With investment fraud, the scammer will lead the victim to invest more and more, sometimes presenting fictitious evidence of enormous gains, before closing out the scam and cutting all contact.

Chinese nationals are arrested on suspicion of running a romance scam out of a huge industrial office park in Indonesia. These large-scale scam centres often present themselves as legal call centres. *© STR/AFP via Getty Images*

Scams using social engineering require significantly more time and resources than simple spamming, but they also have the potential to pay off to a much greater extent. In Ukraine, one estimate judged that socially engineered scams in 2024 were more remunerative than simple online scams by a factor of 14.[3]

Looking ahead, AI's ability to turn vast quantities of personal data into countless individually tailored approaches could result in the distinction between social engineering and spamming becoming increasingly blurred. This could become relevant to mass spear phishing, for instance, where victims receive personalized messages that make use of their own data to achieve credibility. Other tools, such as chatbots informed by large language models, could enable scammers to use AI to undertake some of the work of constructing manipulative relationships with their victims en masse.

One key weathervane of trends in the criminal sphere may be the application of AI in the licit call centre industry, where it is already having a transformative effect on the organization of work. Tellingly, however, there are signs that the human factor still retains considerable power.[4]

The scam toolbox

Lottery scams. Victims are convinced to pay an advance fee to receive a large cash reward. These scams generally involve low levels of social engineering.

Imposter/impersonation scams. These involve a phone call from someone claiming to be a state official, law enforcement officer, bank employee, or other person of authority. Such schemes often create a sense of urgency, pressuring the victim to transfer money to avoid prosecution or even, ironically, fraud.

Investment scams. One of the most sophisticated types, investment scams identify victims with significant assets and, sometimes, a predilection to invest. Over time, the scammer persuades the victim to transfer money, sometimes using deepfakes of celebrities as a lure and fake trading platforms where the victim can watch their 'investment' increase.

Romance scams. The scammer cultivates a romantic connection with their victim before gradually introducing the notion of transferring money, perhaps to buy a property together, facilitate travel, or help with an emergency situation.

'Glocal' force multipliers

Beyond their physical footprint, scam centres make use of six force multipliers that connect the local to the global. These force multipliers essentially form the iceberg of the scam – the massive enabling infrastructure that is hidden from the victim but makes the operation possible.

Networked groups

While some scam centres operate independently, many are part of larger networks. This is in part a result of the easy replicability of the scam centre as a unit – setting up a new site is relatively

straightforward by the standards of organized crime. There are no complicated logistics networks to establish (beyond, potentially, a money laundering apparatus), no turf to secure and little in the way of competition from rival operations. Once a managerial team has scouted out a new location and established a base, local or foreign workers can be hired with relative ease. Software, data and scripts, among other tools, can be bought in through crime-as-a-service (see below).

Today, many scam centres are part of transnational criminal networks that have a presence in several countries around the world and are always looking for new opportunities.[5] Some of these groups also have interests in other forms of organized crime, such as drugs, further blurring the lines between what is considered white collar crime and traditional organized crime. One of the key areas to watch is Latin America, where there is limited understanding of the extent to which major organized crime groups are involved in scam centres.[6]

The networked nature of scam centres brings more professionalization to their activities. Certain functions can be held in common, such as the development and use of technological tools, creating cross-organizational efficiencies. Lessons learned by one branch can be disseminated more broadly throughout the network. The increasing popularity of remote work has also made its way into the world of scamming. Now, it is possible for a scam centre to operate more as a curating force than a physical space: equipped with only a smartphone, a scammer can theoretically work from anywhere in the world, with management delivered remotely.

Networking also enhances the resilience of scam centres. If one scam centre is shut down, the rest of the network (which may well be based abroad) – can continue functioning.

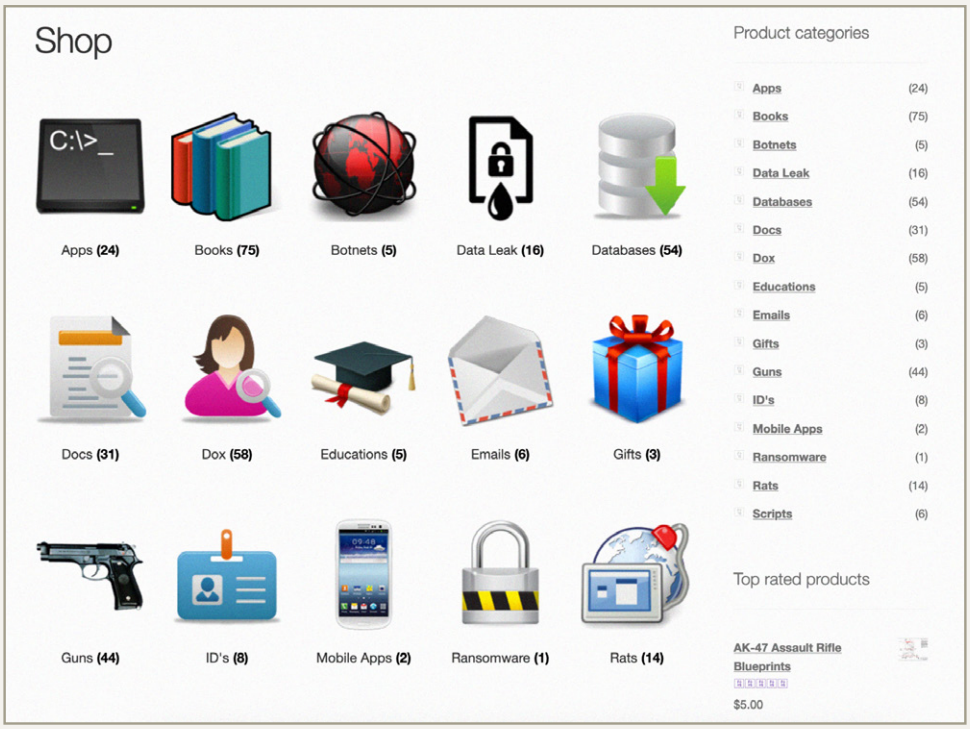
Technology and crime-as-a-service

Ever since scammers adopted the telephone, technology has played a central role in their activities. Today, they can harness a technological arsenal that expands their reach and effectiveness. Voice over internet protocol (VoIP) technology enables scammers to call the world at a fraction of the cost of traditional telephone services, for example, while caller-ID spoofing techniques and VPNs allow them to mask their country of origin. SIM boxes also enable the bypassing of measures designed to block international scam attempts, by providing a bridge to generate a local phone call from abroad.

As discussed above, AI is equipping scammers with a range of capabilities, enabling them to project more convincing deceptions through deepfakes and voice cloning. Common strategies include the impersonation of prominent celebrities, politicians, or even the victim's business colleagues, family or a romantic partner. Behind the scenes, CRM software facilitates the creation of detailed victim profiles, allowing scam centres to marshal the massive data at their disposal and direct it accordingly.

In a grey zone lie the social media platforms that scammers use to connect with victims, either directly or through adverts that are strategically placed by digital marketers to target certain profiles or behaviours (for example, users who have searched for crypto investments). Even when such adverts are taken down, there is often little to prevent scammers from creating new profiles, sometimes with the help of specialized services that supply temporary phone numbers for receiving validation codes, and posting new adverts or contacting new victims.

Crime-as-a-service is also reshaping scam centres in this area. Today, many of the elements that are needed to establish a sophisticated scam centre, from CRM software and scripts to deepfakes and personal data, can be bought online.



Services such as personal data can be purchased on the dark web. *Photo: Screengrab from Dark Net Army*

Money

Like many other forms of organized crime, scam centres have availed themselves of the intricate money laundering apparatus that has emerged to handle illicit proceeds on a global scale. This infrastructure is varied in sophistication, from couriers collecting cash and assets from victims' doorsteps and so-called money mules, whose accounts are used to receive and transmit funds, to over-the-counter crypto exchanges and mixers that seek to sidestep traditional money-tracing tools.

Often a combination of approaches is used to mask the path of stolen money. Funds are moved from bank accounts into cryptocurrency and later cashed out, or expensive assets such as cars and jewellery may be bought and sold on, effectively breaking the chain of traceable transactions. Gambling operations have also played a prominent role in laundering the proceeds of scams in several places.

Law enforcement has made significant strides in this context in recent years, with two notably substantial seizures of illicit proceeds by UK and US authorities in 2025 being traced back to scam centres in South East Asia.[7] These operations against the Cambodia-based Prince Group serve as potent proof that national authorities can successfully tackle the big fish through money-laundering channels. However, it remains to be seen how the large number of smaller outfits, which are still capable of inflicting huge losses, can be disrupted. (The return of scammed money to victims is also an unresolved issue.[8]) Recent responses in Russia, Kazakhstan and elsewhere have focused on increasing the criminal penalties faced by money mules to disrupt this fundamental architecture. This approach is understandable, but given that most criminal organizations treat money mules as entirely disposable, non-core assets, it remains to be seen how effective it will be. Scam centres also have access to many other options for this purpose, and there is no shortage of people who, for a variety of reasons, are willing to loan out the use of their account.

Political protection

Scam centres flourish in contexts where they benefit from political protection. This can take the form of low-level bribes paid to corrupt law enforcement officials in exchange for turning a blind eye, or more structured arrangements. In prison-based scam centres in Colombia, for example, the guards are in effect the organizers of the scheme: they appoint a prisoner to take charge of the yard, who then coordinates the activities of the prisoners carrying out the scams. Revenue is shared on a percentage basis, with the corrupt prison guards pocketing 50% of the takings.[9] In South East Asia, protection for scam compounds appears to be provided by high-level politicians and military personnel.

This political protection not only prevents scam centres from being brought to justice, but also has a corrosive effect on the quality of governance and the rule-of-law in general. As money from crime and state-embedded actors becomes more enmeshed, vested interests grow and back-channel governance verticals form, effectively embedding crime within the functioning of the state. Georgia represents one example of this phenomenon, with several high-level officials having recently been arrested for their involvement in scam centres.[10]

In such contexts, crackdowns should be interpreted carefully. While they may indeed be genuine efforts to dismantle criminal networks, they may also be acts of political theatre, signalling to external actors that the state is taking the issue of scam centres seriously. They could also be strong-arm attempts to remind scammers of the balance of power, or even to negotiate for a share of the profits. Arrests of political figures involved in scam centres should likewise be viewed with caution. While they may represent efforts to clean house, they may also be attempts to target political rivals, enabling a new group of political actors to involve themselves in the illicit economy.

People

Scam centres of every type require a workforce. The simplest arrangements may involve just a handful of people with some phones, an internet connection and a list of numbers. However, more complex operations require a diverse and skilled team to perform a variety of roles.

To fill these positions, scam centres seek employees both locally and internationally. Some are recruited for their skills – language proficiency, for example, or software engineering expertise – while others are hired despite lacking such qualifications. Inmates in prisons or young adults may be attracted by the offer of a job that pays high wages with no experience required, as in Ukraine.

Scam centres also target diaspora communities for various roles. These individuals can serve as local nodes to receive money paid out by scammers, which raises fewer suspicions in the banking system than the sudden transfer of funds abroad. They can also operate as couriers, collecting cash or assets as directed by scammers located in another country. Returning members of a diaspora can contribute excellent language skills and cultural knowledge, helping to boost credibility, as demonstrated by Turkish scammers who have returned to work in Türkiye after time spent in Germany.

Within this labour force, there is broad spectrum of exploitation. Some scammers knowingly and willingly take the work, attracted by the prospect of high earnings, as is the case in Georgia. Others may join without fully understanding the nature of the job, but stay once they have started. Some, however, find that the description of the role they signed up for bears little resemblance to reality. Instead of high wages, they may find that they have a low base salary and must earn most of their pay through commission. Working hours may be long, and the atmosphere pressured and coercive.

At the extreme end of this spectrum are trafficked workers. These people are often recruited from abroad and may travel thousands of kilometres for the job. They may even have paid a broker for the

advertised chance to earn much higher wages than they would at home. When they arrive, however, they find a very different situation. Some become trapped in debt bondage. Others are deprived of their liberty and are sometimes subjected to extreme torture. This has been widely documented in South East Asia, where trafficked workers in scam compounds find themselves in a situation from which there is little hope of escape. Murder and suicide are common.[11] And such practices are by no means restricted to South East Asia. Reports of coercive and violent behaviour have also emerged from Ghana, the United Arab Emirates, Nigeria, Ukraine and Pakistan.[12]

This has created a complex situation in which the perpetrators of the scams have also been victimized. The ramifications are particularly stark in cases involving trafficked scammers who are freed from compounds and return home. While they may not have engaged in scamming willingly, they often find that their criminal past casts a shadow over their search for legitimate employment. China, for instance, has indicted tens of thousands of people for online scamming after their repatriation from South East Asia. If these former perpetrators cannot secure gainful employment, they may turn back to scamming. Cases of repatriated scammers returning to their former activities have already been evidenced in India and China.[13]

It is important to note that these forms of experience are not mutually exclusive. Scammers may move between categories, becoming the willing party and then the exploited party, or vice versa. This makes delineating victim protection and criminal responsibility even more challenging, underlining the necessity of comprehensive victim identification systems.

Geopolitics

Scammers are highly attuned to the opportunities afforded by geopolitical events, and are quick to capitalize on confusion and chaos. The coronavirus pandemic, for instance, triggered a major surge in scamming activity, as work and commerce shifted almost entirely online.[14] The Russo-Ukrainian War provided a further catalyst, prompting the development of new schemes such as fraudulent crowdfunding for military equipment, fake claims of aid from international organizations, demands for 'rescue fees' to locate missing relatives, and impersonation scams accusing victims of collaboration with the enemy – allegations that are 'resolved' through payment.[15]

More broadly, the increasingly fractured geopolitical landscape also provides scammers with protection. A lack of law enforcement cooperation between countries enables scammers to operate without fear of repercussions. In some cases, this manifests as a pseudo-political practice known as 'patriotic scamming', whereby scammers deliberately target victims in 'enemy' countries that lack the capability or diplomatic relations to trace their activities. This has been documented in Ukraine and Pakistan.[16] More generally, scam centres may adhere to the long-standing cybercrime rule that states you should never target victims in your home country, to avoid internal law enforcement attention. This pattern has been observed in at least one criminal network in Eurasia, while Chinese authorities have felt compelled to launch public education programmes reminding citizens that scamming foreigners is also a crime.[17] As deglobalization advances, these cooperation fissures may only widen, and new ones may emerge, creating more and more safe harbours for scammers.

A related point concerns the rise in authoritarianism in many countries worldwide and the concomitant shrinking of civic and journalistic space, which often plays a leading role in exposing the practices and activities of scam centres. As with all forms of organized crime, scam centres benefit from staying in the shadows; if independent scrutiny diminishes, and criminal relationships are forged with corrupt state actors, the activities of scam centres will be difficult to map and the perpetrators difficult to dislodge.

TOWARDS A 'WHOLE PROBLEM' RESPONSE

As the above analysis demonstrates, scam centres are a unique and highly sophisticated form of organized crime that is deeply connected to the sinews of the modern information age and present-day geopolitical shifts. They exist in various shapes and sizes, and employ different business models, but all share a common use of six glocal force multipliers.

Bearing this in mind, it is possible to identify the 'ingredients' that comprise a scam centre (Figure 1). This template reveals that, despite their differences in practice, all scam centres have discernible shaping factors, such as their physical footprint, their use of a workforce and their ability to secure local protection.

This lens can help broaden the focus, enabling a shift away from reactive enforcement towards a more holistic, systems-orientated approach. Adopting lessons from other forms of transitional organized crime that focus on upstream disruption and targeting the enabling infrastructure will pay dividends, and indeed many such efforts are already underway. But it is also necessary to design 'whole problem' responses, incorporating all facets of the scam centre ecosystem. Otherwise, no matter how many scam centres are taken down, the ground will still be fertile for new actors to step in.

The recommendations below form part of a move towards this comprehensive response. They are aimed at creating a broad spectrum of activities that compromise the operating environment of scammers on several levels. (Further details of these and other recommendations can be found in 'A world of deceit: Mapping the landscape of the global scam centre phenomenon, published by the GI-TOC in March 2026.)

Harmonize tools of leverage

Improved coordination among law enforcement agencies dealing with scam centres globally may itself act as a force multiplier, not least since many investigations may be targeting the same criminals. By pooling resources, knowledge and leads, law enforcement should be able to build cases and execute investigations faster and more efficiently. Countries affected by scamming may also have diplomatic

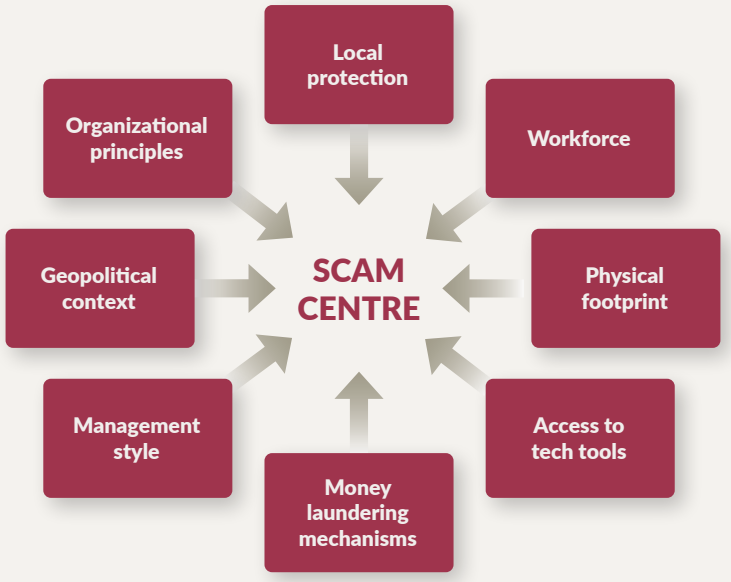


FIGURE 1 'Ingredients' of a scam centre.

and economic tools at their disposal to put pressure on countries where strong political protection allows scam centres to operate. Countries can also seek to revise their domestic legislative approach to increase accountability with regard to the tools commonly used by scammers, including social media, financial services and other forms of technology. That said, it is imperative to balance greater control of communication technologies with concerns for civil rights.

Improve international cooperation

Scammers take advantage of political divisions, both in the content of their scams and in how they operate. Where there is a lack of cooperation between countries, scammers can work with effective impunity. Improving cooperation between countries may be extremely challenging in certain contexts, but collaboration on a case-by-case basis could be mutually beneficial, and help close a loophole currently exploited by organized crime.

Create new thinking for new challenges

AI is a game-changer for scammers. Deepfakes, fake apps and voice cloning, among other tools, all bestow a high level of credibility to scams, being extremely difficult to distinguish from the real thing. Auto-translation and large language models can also help automate, to a point, processes that would formerly have required a sizeable workforce. As scam centres enter their next stage of sophistication and expand to other forms of cybercrime, new tools and strategies will need to be devised that harness the skills and expertise of a range of stakeholders, including technology firms, law enforcement agencies, governments and civil society. Increasing safeguards, public awareness campaigns and defensive AI tools that can protect against this new wave scams will all be necessary.

Reintegrate former scammers

Scam compounds in South East Asia have been reported as exploiting hundreds of thousands of people. Today, tens of thousands of these workers are returning home, where they may find that their past as a scammer – even if coerced – may act as a barrier to re-entering the legal workplace. Given their skills and experience, it is critical that alternative employment pathways are established to prevent former trafficked scammers from falling back into fraud, either by joining existing networks or setting up their own operations.

Scammers who have not been trafficked also pose a skills proliferation risk, as they may seek to use their abilities and experience of working in scam centres when back home. Given their willing involvement in scamming, providing them with enhanced economic opportunities may be neither appropriate nor effective. In many places, the licit economy will be unable to match the earnings potential of illegal activities. The most appropriate form of intervention to prevent these individuals from reoffending will have to be decided on a case-by-case basis. International law enforcement cooperation is essential to build the data picture of such individuals and share intelligence.

Ultimately, monitoring who comes home, and what skills and profile they have, will be essential to formulating an appropriate response, ranging from rehabilitation and support to monitoring and potential indictment.

NOTES

1 For a full analysis of the issues covered in this policy brief, including country examples, see Kristina Amerhuaser and Alex Goodwin, A world of deceit: Mapping the landscape of the global scam centre phenomenon, GI-TOC, March 2026, https://globalinitiative.net/analysis/mapping-global-scam-center-phenomenon/; and Alex Goodwin, Scammers' paradise? Assessing scam centres in Eurasia, GI-TOC, April 2026.

2 Sam Rogers, International scammers steal over $1 trillion in 12 months in global state of scams report 2024, GASA, 7 November 2024, https://www.gasa.org/post/global-state-of-scams-report-2024-1-trillion-stolen-in-12-months-gasa-feedzai; Global GDP was estimated at US$111 trillion in 2024, meaning US$1 trillion is equivalent to 0.9%. See Statista, Global gross domestic product (GDP) from 2000 to 2030 (in trillion US dollars), https://www.statista.com/statistics/268750/global-gross-domestic-product-gdp/.

3 Ukrainian Interbank Payment Systems Member Association (EMA) presentation shared with the GI-TOC, February 2025.

4 McKinsey, The contact center crossroads: Finding the right mix of humans and AI, 19 March 2025, https://www.mckinsey.com/capabilities/operations/our-insights/the-contact-center-crossroads-finding-the-right-mix-of-humans-and-ai.

5 See, for example, the recent entrance of an East Asian syndicate into Batumi in Georgia: UNODC, Inflection point: Global implications of scam centres, underground banking and illicit online marketplaces in Southeast Asia, April 2025, https://bit.ly/4iqcYll.

6 In Colombia, for instance, prison scammers typically impersonate members of high-profile armed groups, resulting in victims mistakenly claiming that the threats were made by cartels or guerrilla groups. A similar situation applies in Brazil, where scammers often pretend to be affiliated with major organized crime groups such as the First Capital Command (PCC). As a result, media reports often claim that scam centres are run by major cartels. Interview with police investigator of the São Paulo civil police fraud division, September 2025; interview with the Attorney General's office, Bogotá, January 2026.

7 Erin Hale, UK sentences Chinese scammer after record-breaking Bitcoin seizure, Al Jazeera, 12 November 2025, https://www.aljazeera.com/news/2025/11/12/uk-sentences-chinese-scammer-after-record-breaking-bitcoin-seizure; Matt Burgess and Andy Greenberg, Feds seize record-breaking $15 billion in Bitcoin from alleged scam empire, Wired, 14 October 2025, https://www.wired.com/story/feds-seize-record-breaking-15-billion-in-bitcoin-from-alleged-scam-empire/.

8 Spencer Woodman, Questions swirl around US plans for record $15B Prince Group crypto seizure, International Consortium of Investigative Journalists, 18 March 2026, https://www.icij.org/investigations/coin-laundry/questions-swirl-around-us-plans-for-record-15b-prince-group-crypto-seizure/.

9 Research undertaken by C-Análisis shared with the GI-TOC, December 2014.

10 See, for instance, OCCRP, Georgia detains ex-security chief over alleged bribes tied to global scam call centers, 23 December 2025, https://www.occrp.org/en/news/georgia-detains-ex-security-chief-over-alleged-bribes-tied-to-global-scam-call-centers.

11 GI-TOC, Compound crime: Cyber scam operations in Southeast Asia, May 2025, https://globalinitiative.net/analysis/compound-crime-cyber-scam-operations-in-southeast-asia/.

12 See Kristina Amerhuaser and Alex Goodwin, A world of deceit: Mapping the landscape of the global scam centre phenomenon, GI-TOC, March 2026, https://globalinitiative.net/analysis/mapping-global-scam-center-phenomenon/.

13 Jason G Tower, Exporting fraud: China's acquiescence to Myanmar's military regime fuels 'foreigner butchering' scam epidemic, GI-TOC, 10 October 2025, https://globalinitiative.net/analysis/chinas-acquiescence-to-myanmars-military-regime-fuels-foreigner-butchering-scam-epidemic/; interview, New Delhi, December 2025.

14 Tuesday Reitano and Mark Shaw, *Criminal Contagion: How Mafias, Gangsters and Scammers Profit from a Pandemic*, Hurst Publishers, 2021.

15 Nikolai Kireev, Telephone scams in 2023, Finance.ua, 9 March 2023, https://finance.ua/ua/goodtoknow/telefonni-szahrajstva-2023; Office of the Prosecutor General of Ukraine, Relatives of military personnel who went missing or were captured were defrauded of UAH3 million – a group of individuals was exposed in the Dnipropetrovsk region, 3 June 2025, https://www.gp.gov.ua/ua/posts/osukali-na-3-mlngrn-rodiciv-viiskovix-yaki-znikli-bezvisti-ci-potrapili-v-polonna-dnipropetrovshhini-vikrito-grupu-osib; Mykola Tyshchenko, Ботоферма обікрала на 7,5 мільйонів гривень матір Героя, що загинув, захищаючи Україну, Telegram, https://t.me/NikolayTishchenko/1789; Polina Snezhina, Man who defrauded the mother of a deceased soldier of almost UAH150 000:imprisoned man to be tried in Zaporizhia, Suspilne, 17 June 2025, https://suspilne.media/zaporizhzhia/1045025-osukav-matirzagiblogo-vijskovogo-majze-na-150-tis-grn-u-zaporizzi-suditimutuvaznenogo-colovika; Anastasia Chebrets, 'Agent Nimets' and its call centre 'E-Scam' in Lviv, Informator, 6 September 2023, https://informators.press/ahent-nimets-i-yoho-kol-tsentr-ye-shakhraystvo-u-lvovi/; How scammers steal military fees: common schemes, Espresso West, 29 February 2024, https://zahid.espreso.tv/kryminal-nadsilatigroshi-lishe-tomu-komu-doviryaemo-yak-shakhrai-kradut-zboridlya-viyskovikh-i-privlasnyuyut-sobi-groshi; Oleg Bessarab, Fraudsters in Ukraine have come up with a new scheme, intimidating with treason – police, UA.News, 18 May 2025, https://ua.news/ua/ukraine/shahrayi-v-ukrayinyprydumaly-novu-shemu-zalyakuyuchy-derzhzradoyu-politsiya.

16 Alex Goodwin, Scammers' paradise? An assessment of scam call centres in Eurasia, GI-TOC, April 2026; Dwaipayan Ghosh, Fraud calls from Pakistan numbers rise amid new malware threat, *Times of India*, 13 May 2025, https://timesofindia.indiatimes.com/city/kolkata/fraud-callsfrom-pakistan-numbers-rise-amid-new-malware-threat/articleshow/121143100.cms.

17 Jason G Tower, Exporting fraud: China's acquiescence to Myanmar's military regime fuels 'foreigner butchering' scam epidemic, GI-TOC, 10 October 2025, https://globalinitiative.net/analysis/chinas-acquiescence-to-myanmars-military-regime-fuels-foreigner-butchering-scam-epidemic/.

GLOBAL INITIATIVE
AGAINST TRANSNATIONAL ORGANIZED CRIME

ABOUT THE GLOBAL INITIATIVE

The Global Initiative Against Transnational Organized Crime is a global network with 800 Network Experts around the world. The Global Initiative provides a platform to promote greater debate and innovative approaches as the building blocks to an inclusive global strategy against organized crime.

www.globalinitiative.net