STIMSON

PRESIDENTIAL INBOX MEMO

Cyber & Southeast Asia Programs

Countering Cyber Scam Operations Project

November 2024

To protect Americans, prioritize countering cyber scam operations in the Indo-Pacific

By Brian Eyler, Allison Pytlak, Courtney Weatherby and Shreya Lad

TOPLINE

Cyber scams targeting American citizens are a national security threat that demands a whole-of-government approach and coordination between the United States and its allies and partners who are similarly targeted.

Cybercrime operations run out of scam compounds in the Indo-Pacific should be a priority for the Trump administration. A growing number of Americans are victimized by online scams and fraud, and the global profits from these criminal operations exceed those of other illegal activities —including global illicit drug trafficking.

The current approach to preventing, detecting, and responding to cybercrime scams is insufficient. It allows criminal networks to misuse U.S. digital and financial institutions, alienates victims of scams, and allows adversaries to benefit from illicit activity. The new administration should counter cyber scams through a coordinated approach centered around a national command center, improved interagency collaboration on cybercrime, partnership with regional allies that are trying to crack down on scam compounds in their countries, and public awareness campaigns around this growing threat.

stimson.org 202.223.5956

WASHINGTON 1211 Connecticut Avenue, NW 8th Floor 20036

THE PROBLEM

Americans are increasingly targeted by online scams, with rapidly rising numbers of damaging investment fraud and romance/confidence scams reported since 2018. A study by the Global Anti Scam Alliance and Feedzai estimates that nearly a quarter of Americans were scammed in 2023, and collective losses reached $159 billion USD, or approximately 0.6% of GDP. The number of individuals that have lost their life savings and homes to cyber scam operations run by transnational criminal groups overseas is growing.

Many of these criminal networks house operations inside scam compounds located in Indo-Pacific countries such as Cambodia, Laos, Myanmar, and the Philippines. Scam compounds are a complex crime zone, acting both as secured areas in which criminal organizations coordinate and run scam operations, as well as a venue for modern slavery. Most of the 'workers' inside are lured into false work situations, held against their will, and forced to participate in criminal activity.

Cybercrime scam operations thus present a challenge to United States (U.S.) and allied interests in the Indo-Pacific, threatening to undermine governance, rule of law, and human rights in the countries where they are located, with knock-on effects and costs borne by key victim economies in the region including Australia, Thailand, and Vietnam. Online scam operations also have a growing role in strategic competition with China and North Korea, amplifying the disruptive potential of cyber scams for the United States.

Despite the scale of the problem, the U.S lacks a coordinated effort to counter cyber scam operations and protect vulnerable Americans. Over the last few years U.S. government agencies including the Department of Justice, Federal Bureau of Investigations (FBI), the National Security Council, and the State Department have turned more attention to the issue, but there is no single agency with sufficient resources and a mandate to adequately coordinate interagency efforts on this issue.

ESSENTIAL CONTEXT

The perpetrators

With rapidly growing war chests and increasingly sophisticated methods of evasion, powerful criminal networks can co-opt political actors and fuel corrupt activities in countries across the Indo-Pacific, particularly Cambodia, Laos, and Myanmar. Many of these groups are also engaged in other illicit activities such as drug trade and human trafficking. Globally, sophisticated criminal networks are now earning $3 trillion annually from scams and fraud, far outpacing income earned by the global illicit drug trade. High profit margins and relatively low risks motivate many criminal groups to

invest in cyber-scam operations and cryptocurrency, which also improves their ability to launder funds from other illegal activities such as drug or human trafficking.

Many of these networks are Chinese in origin. The actors responsible for some of the biggest cryptocurrency scams in Southeast Asia are linked with entities sanctioned by the U.S. Global Magnitsky Program such as the Golden Triangle Special Economic Zone run by sanctioned Chinese national Zhao Wei and North Korean cyber threat actor Lazarus Group, known to help the regime evade U.S. sanctions and illicitly finance its weapons of mass destruction program.

China is active in combatting cyber scam compounds given that many of the transnational criminal groups are Chinese and target Chinese nationals, but its efforts primarily aim to reduce targeting of its citizens as victims of scams and trafficking. As a result, Chinese activities are driving criminal groups to target English-speaking countries and other nationalities across the Indo-Pacific. The People's Republic of China's recent crackdowns on scam compounds in Myanmar have simply driven scam operations to relocate and shift their target profile.

The victims

Hundreds of thousands of people from more than two dozen nations are illegally and unwittingly trafficked into countries in the Indo-Pacific where they are forced to scam against their will. Those who resist face torture, physical abuse, or being sold to other operation centers. Trafficked workers are often young, educated professionals with language or relevant IT skills, often lured by false job advertisements and facing economic pressure at home.

In the U.S. and countries like Australia, Canada, and the U.K., the toll of romance and investment scams on lives and livelihoods is breaking new thresholds and is increasingly a topic covered by major media outlets. Victims often describe the intense shame they feel in having been scammed, which contributes to under-reporting, and some tragically decide to take their lives. Others live in destitution after losing significant life or retirement savings to such scams, posing a long-term cost to social security and other national expense rolls. There is, currently, little potential for legal recourse or compensation given the international nature of the criminals and the often-technical nature of the crime.

The gaps

In the U.S., state and local enforcement agencies often turn down or ignore victims of cyber-crime due to a lack of investigative capacity, limited mandate to prosecute cybercrime, and a lack of awareness of the sprawling scale of this issue. Currently even basic data about the types and approaches for fraud in the United States is not widely available. A range of different agencies at the federal, state, and local levels—the FBI's

Internet Crime Complaint Center, Federal Trade Commission's Report Fraud, Consumer Financial Protection Bureau, local police, as well as individual service providers in finance and telecommunications—are all points of contact for victims trying to report scams or fraud. According to the 2024 State of Scams Report from the Global Anti-Scam Alliance, fraud and scams are the most experienced crime in the United States. Inability of government and service providers to effectively respond—especially in cases with significant losses—erodes trust.

This is a long-term challenge for the digital economy, including for major emerging and rapidly growing industries such as cryptocurrency and artificial intelligence (AI). A large percentage of total scam revenue comes from the theft of digital assets, and most investment scams use cryptocurrency platforms and wallets as a venue for accessing and stealing funds. This has also held back the U.S. cryptocurrency industry amid regulatory confusion, and the use of digital assets for fraud. Bad actors are also increasingly adept at using new technologies like generative AI and deepfakes for online scamming and fraud. These industries—particularly AI with its transformative potential—could also face reputational or legal risk without better regulation and risk management.

The absence of clearly defined, unambiguous regulations and best practices for risk management has left the cryptocurrency industry more vulnerable to fraud, scams, and the misuse of digital assets. Industry executives have called for legislation that protects users from fraud and crypto-enabled cyber scams. There is a need for the U.S. government to more actively engage with industry to forge a path forward to avoid further erosion of trust in key new technologies and the digital economy.

POLICY RECOMMENDATIONS

An effective approach to countering scam operations should include a centralized mechanism to detect scams, address the use of financial platforms to conduct scams, prevent the victimization of forced scammers and scam victims, and detect and mitigate the threat at its source with the support of U.S. allies and partners. The incoming administration should consider the following:

Create a national scam center responsible for centrally tracking scam reports, providing victim support, and coordinating with law enforcement on appropriate responses.

- Bring representatives of multiple government agencies and key industry actors together in a common body that can streamline response and improve data collection.

- Establish a national dataset to centralize reporting across state lines and federal agency silos. This would allow for better understanding and analysis of the most common tactics used by scammers and thus identify low-hanging technical preventions and responses that regulators, businesses, and consumers can take.

- Congress should commission a study on the role of cryptocurrency exchanges, with input and consultation from relevant stakeholders including the cryptocurrency industry and private sector. This study should aim to bring clarity around mandates, roles, and responsibilities for cryptocurrency regulation among relevant entities in relation to the scam operations issue.

Coordinate with allies and partners including Australia, Canada, Singapore, Japan, South Korea, Thailand, the Philippines, and the United Kingdom to improve information-sharing to avoid a "whack-a-mole" approach to shutting down scams.

- Adopt a comprehensive prevention and detection strategy rather than relying on responding to problems as they arise.

- Facilitate the use of treaties on Mutual Legal Assistance in Criminal Matters (MLATs) which are helpful for sharing evidence to prosecute transnational cyber criminals and overcome jurisdictional barriers, but they are time consuming and difficult to obtain. Broader agreements like the recently adopted UN Cybercrime Treaty, or regional arrangements such as through ASEAN, may offer new avenues for information- and evidence-sharing.

- Better leverage mechanisms like INTERPOL for information and intelligence-sharing with international partners.

- Technological solutions to prevent scamming, such as through cooperation with telecommunications or banking companies, are worth exploring but with due regard for personal privacy rights. Industry actors can lead on identifying ways to share key but non-sensitive data among other users.

Provide technical and capacity support to countries hosting scam centers and compounds to reduce instances of cybercrime and breakdown criminal networks.

- Utilize the Mekong-U.S. partnership as a platform for regional coordination, technical training, and capacity-building with countries that are hosts to scam compounds (particularly Cambodia, Laos, and Myanmar).

- Engage directly with regional neighbors who are similarly targeted by scams or forced labor to establish shared protocols and responses, including but not

limited to Thailand, Vietnam, Singapore, and other partners in the Indo-Pacific.

- USAID can conduct bilateral activities to combat trafficking in persons (TIP) in host countries, and build capacity on legal issues, in line with the Agency's 2023-24 digital strategy.

- Create agency-to-agency partnerships between the U.S. and partner countries' law enforcement agencies. These have, in the past, been useful for combatting telecommunications scams and for information-sharing. This model can offer assistance, fill capacity gaps, and open pathways for the arrest and prosecution of criminal actors who stole from Americans. Such collaboration can also allow border checkpoints in key countries to be more prepared to combat TIP at their borders.

Institute public awareness-raising campaigns to prevent future victims and destigmatize the problem.

- Campaigns like "Stop, think fraud!" in the United Kingdom offer examples of government-led approaches which could be adapted and implemented in the United States to raise awareness among potential victims.

- Private sector actors like social media and cryptocurrency companies also have a vested interest in ensuring that their services remain trusted by consumers, and there are opportunities to collaborate with key private sector actors on targeted awareness raising campaigns for those most likely to be victimized.

- The U.S. intelligence community with the Department of Justice should improve awareness among key law enforcement agencies of how these cybercrimes unfold and improve recognition that those reporting scams and fraud are victims of a crime. Campaigning should be inclusive, especially since scammers typically target English and Chinese speakers. This will help destigmatize reporting and can improve victim support networks.