



INTERPOL

FORGED REALITIES:

CONFRONTING THE THREAT OF SYNTHETIC MEDIA IN SOUTHEAST ASIA

RESEARCH STUDY
AUGUST 2026



Project funded by the
Government of Japan

TABLE OF CONTENTS

FOREWORD	3
ACKNOWLEDGEMENTS	4
DISCLAIMER	5
EXECUTIVE SUMMARY	6
1. INTRODUCTION	7
1.1. Methodology	8
2. SYNTHETIC MEDIA THREATS IN SOUTHEAST ASIA	10
3. LAW ENFORCEMENT RESPONSE TO SYNTHETIC MEDIA THREATS	15
3.1. Tools	15
3.2. Reporting systems and awareness campaigns	16
3.3. Competence enhancement	19
4. RECOMMENDATIONS	21
5. ROLE OF INTERPOL	23
6. CONCLUSION	24

FOREWORD

Artificial intelligence (AI) has become more pervasive in our day-to-day lives, enabling easily accessible platforms to provide opportunities for straightforward and speedy completion of tasks and creation of content disseminated on digital devices. However, with generative AI platforms' accessibility and ease of use, criminals now have a multitude of opportunities to amplify their approaches to tricking, threatening, robbing, and abusing victims.

This publication highlights the threats of synthetic media in the Southeast Asian region and aims to shed light on the evolution of a crime landscape that continues to grow on a global scale. It illustrates different kinds of synthetic media threats and presents examples of how law enforcement agencies in Southeast Asia respond to them with existing laws. With its diverse set of regulations, Southeast Asia provides an interesting lens for different gradients of environments and threat developments requiring specific approaches.

As the world's largest law enforcement organization, INTERPOL aims to support member countries around the globe in understanding crimes as early as possible, being at the forefront of analysing how a threat emerges and evolves. My hope is that this publication would serve as an instigator for all member countries to define and examine similar synthetic media threats, and stop the harm caused by synthetic media.

Apart from identifying these threats, this research study also points out tools, reporting mechanisms, awareness campaigns, and skills enrichment used by law enforcement agencies in detecting and investigating synthetic media threats, and is relevant and applicable to synthetic media-enabled threats regardless of crime categories. This is a testament to the need for a multi-layered approach to an issue that seemed to emerge in such a rapid manner.

I am grateful for the support of the Government of Japan in ensuring that law enforcement agencies are enhancing their knowledge and capabilities in the area of synthetic media threats through Project SynthWave, the pillar which underpins this research study. INTERPOL supports member countries in addressing technology-enabled cross-cutting threats and crimes that are borderless and at risk of being boundless.

While law enforcement agencies face challenges unique to their national contexts, we all share a common goal – protecting our communities from harm. Understanding any type of crime begins with a step, similar to this research study, and progresses with the continuous examination of an ever-changing global landscape. This is only the beginning of an in-depth, multi-layered, and international-law-enforcement approach to detecting and fighting synthetic media threats together.



安部俊伸

Toshinobu Yasuhira
Director, Innovation Centre
Executive Directorate Capacity Building and Innovation
INTERPOL

ACKNOWLEDGEMENTS

INTERPOL would like to thank the Government of Japan for their generous support of Project SynthWave, under which this research study was compiled. This research study was created through extensive consultations with law enforcement agencies from across Southeast Asia. INTERPOL would like to thank the law enforcement agencies from the participating countries of Project SynthWave, namely Brunei, Cambodia, Indonesia, Laos, Malaysia, Philippines, Singapore, Thailand, and Viet Nam for their active participation in the project's activities which led to the compilation of this study. INTERPOL would like to additionally thank the Cambodian National Police, the Ministry of Public Security of Laos, the Ministry of Public Security of Viet Nam, the Royal Brunei Police Force, the Royal Malaysian Police, the Royal Thai Police, and the Singapore Police Force for contributing to this study through virtual meetings and questionnaire responses. We would also like to extend a special thanks to the Philippine Center on Transnational Crime, the Philippine Department of Justice – Office of Cybercrime (OOC), civilian groups from the Philippines, Armed Forces of the Philippines Cyber Group (AFPCG), and several agencies within the Philippine National Police including the Cybercrime Investigation and Coordinating Center (CICC), the Department of Information and Communications Technology (DICT), the Philippine National Police Cybersecurity Operations Centre (CSOC), and the Philippine National Police Cyber Response Unit for contributing to this study through in-person meetings and roundtables.

From the private sector, INTERPOL would like to thank Mr Itaru Ueda, Assistant Manager, Cyber Security Strategy Department, NEC Corporation for his invaluable research and contributions to this study. INTERPOL would also like to thank Mr Roel S. Reyes, Senior Threat Researcher, Trend Micro Inc. and Ms Lyantoniette Chua, Founder, Asia Affairs AI (AAA), for contributing to this study through in-person and virtual consultations. INTERPOL is grateful to Ms Helena Yixin Huang, Associate Research Fellow, S. Rajaratnam School of International Studies, Nanyang Technological University, and Mr Nikolai Suhharnikov, Head of Technical Pre-Sales, Sumsu, for their valuable and insightful peer review of this study.

Finally, we would like to thank the National Police Agency (NPA) Japan and the Japan Cybercrime Control Center (JC3) for co-hosting the INTERPOL Conference on AI in Digital Forensics: Unpacking Insights in Investigations and Analysis which took place in October 2025 in Tokyo. The insights derived from this conference were used to enhance this study.

INTERPOL is committed to supporting law enforcement in understanding, preventing, and combating the threats posed by synthetic media technology by enhancing our global research efforts, facilitating knowledge sharing, developing resources, and undertaking competence enhancement efforts.

DISCLAIMER

This research study offers general information and guidance on understanding and approaching the threats of synthetic media in the Southeast Asian region, and how law enforcement agencies may respond to them. The information in this research study is obtained from member countries, private partners, and open sources, and is provided for the consideration of readers at their discretion.

The examples, descriptions and discussions in this research study are intended as options for consideration, rather than as recommendations, encouragement or definitive proposals. References to external links, publications or any actions, proposals, measures, or policies developed on the basis of this research study must be taken with reference to the applicable laws as verified and tested in the relevant jurisdictions by the relevant readers. INTERPOL bears no responsibility in respect of any such actions, steps, measures, or any documents created based on this research guide.

Links to external publications or websites included in this research study are provided as references only, and do not constitute an endorsement by INTERPOL of those publications or their content. It is the responsibility of the user to evaluate the content and usefulness of information obtained from such other publications/websites.

INTERPOL does not endorse or recommend any product, process, or service. Therefore, mention of any products, processes, or services in this research study cannot be construed as an endorsement or recommendation by INTERPOL.

Descriptions of the provisions of certain legal instruments in this document are presented as discussions only and are not, nor may be construed as, proposals on applicable interpretations in respect of any of these legal instruments.

This research study has not been formally edited. The content of this publication does not necessarily reflect the views or policies of INTERPOL, its member countries, its governing bodies, or contributory organizations, nor does it imply any endorsement.

Although this study does not contain law enforcement information, it should still be considered sensitive and should be protected from unauthorized access, and should only be used for law enforcement purposes. Any further dissemination of this content is restricted to official law enforcement authorities for legitimate law enforcement purposes. This information may be used solely by national law enforcement agencies for information and international police cooperation purposes, may only be used for intelligence purposes, and should not be construed as being a document of evidential value or for use in judicial proceedings. Any decision on action to be taken based on this information is within the discretion and responsibility of the appropriate national law enforcement authorities and should be done in accordance with the applicable national law and international obligations of the country concerned. The written permission of the INTERPOL Innovation Centre is required in order to disseminate this document or any part of it.

EXECUTIVE SUMMARY

This research study examines the rise of synthetic media threats in Southeast Asia, outlining the different types of threats, analysing law enforcement responses to the criminal misuse of the technology, and presenting key recommendations.

The most prominent synthetic media threats in the region include: (1) synthetic identities for digital fraud; (2) non-consensual pornography; (3) disinformation; and (4) creating and disseminating malware at scale, with the latter being an emerging yet nascent threat with the potential to escalate in the future. In order to promote a preventative approach to synthetic media misuse, governments and law enforcement agencies have launched awareness campaigns, with some agencies issuing statements and using their websites and social media channels to raise public vigilance against emerging criminal modus operandi. Some law enforcement agencies in the region actively offer learning opportunities regarding synthetic media detection and investigation to their officers, while most remain in the early stages of such competence enhancement efforts due to the lack of resources and expertise. Law enforcement has also built partnerships with academia, industry, and civil society for several aspects of response, including acquiring detection tools and developing learning opportunities. Furthermore, the borderless nature of synthetic media crime makes robust international and regional law enforcement cooperation essential.

In view of escalating synthetic media threats and current law enforcement response, the study also highlights the following key recommendations for law enforcement.

- **Competence enhancement:** there is a critical need to promote learning opportunities on synthetic media to all criminal justice actors to aid: (1) all law enforcement officers in their understanding of the technology and handling of citizen reports; (2) specialists in effectively detecting and investigating synthetic media content; and (3) judges and prosecutors in understanding related evidence and chain-of-custody procedures when dealing with such cases in court.
- **Guidelines:** clear guidelines and taxonomy must be established for: (1) the classification of AI-generated material, outlining the response for each degree of harm, including protocols for cooperation with private sector partners; and (2) the admissibility of AI-enabled evidence in court.
- **Partnerships:** law enforcement must build robust partnerships to: (1) leverage the expertise of private sector to develop tools and learning opportunities; (2) ensure that multisectoral expert groups are created across law enforcement, industry, and academia to share latest information on synthetic media threats and response mechanisms; and (3) foster interagency regional and international cooperation, which is imperative for collaborative action and the sharing of best practices.

Finally, the study concludes that building resilience against synthetic media warrants a collaborative approach within the international law enforcement community and highlights the role of INTERPOL in promoting community building, knowledge sharing, and cooperation to help law enforcement combat synthetic media threats.

1. INTRODUCTION

The rapid advancement of artificial intelligence (AI) has created a dual effect for law enforcement who are leveraging this technology for their daily work while also grappling with its criminal exploitation. Malicious actors use AI to carry out sophisticated, borderless crimes, often leaving law enforcement in a reactive state. Synthetic media are one such AI-enabled technology that are increasingly being misused by criminals.

Synthetic media refer to the type of media content, such as images, videos, audio, or text that have been completely or partially generated or manipulated using AI algorithms.¹ Arguably, the most prominent subset of this technology from a law enforcement lens is deepfake technology, which refers to AI-generated or manipulated image, audio, or video content that resemble existing persons, objects, places, entities, or events and would falsely appear to a person to be authentic or truthful.² Apart from deepfakes, synthetic media also encompass AI-generated text, including disinformation, AI-driven bot-generated content, and other forms of algorithmically produced material that may be used to deceive, manipulate, or mislead.³

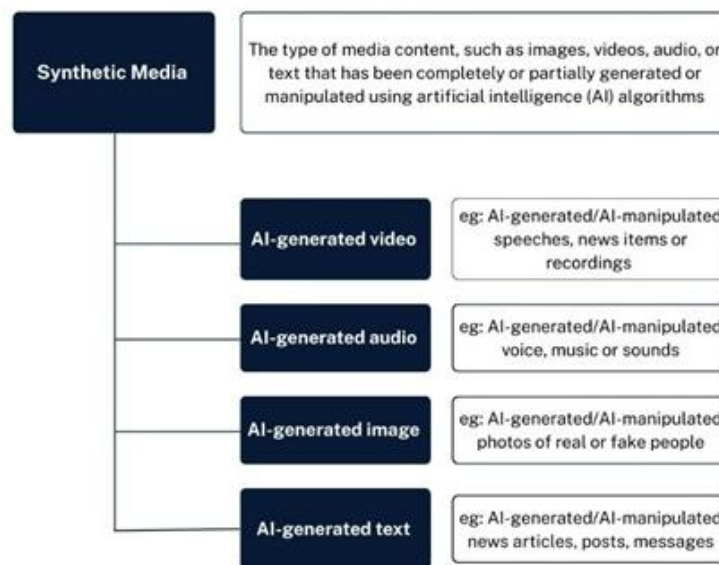


Figure 1: Components of synthetic media technology

Since the advent of the first deepfake in 2017⁴, this technology has evolved significantly, contributing to a range of crimes including financial crime, identity theft, child sexual abuse, and disinformation. For instance, in 2024, UK law enforcement arrested a man who used synthetic media technology to transform real images of children into deepfake pornography, with victims and accomplices located across multiple countries.⁵ Such cases highlight the borderless nature of synthetic media crime and its ability to amplify existing threats through sophisticated technological methods. Additionally, the rise of synthetic media has not only expanded avenues for criminal activity, but also complicated the process of verifying the legitimacy of evidence and maintaining chain-of-custody. While synthetic media can be used to fabricate evidence, they can also give rise to a phenomenon known as “liar’s dividend”, wherein the authenticity of real evidence can be called into question, citing AI-enabled manipulation.⁶ An example of this

phenomenon was seen in a case where a defence team suggested that a video submitted as evidence by the plaintiffs could be a deepfake, arguing that the individual in the video was a public figure and the subject of multiple AI-generated videos.⁷

With the rapid evolution of synthetic media technology, law enforcement has been addressing its advancing misuse by developing and acquiring detection tools, and building partnerships to leverage the expertise of industry, academia, and civil society. Nonetheless, with synthetic media advancing rapidly, these efforts need to be further amplified to effectively deal with the criminal use of this technology. Additionally, given the transnational nature of synthetic media crimes, regional and international law enforcement cooperation is essential to ensure a coordinated and effective response to the malicious use of this technology.

With an internet penetration rate of 70-80 per cent as of 2023,⁸ Southeast Asia has emerged as a testing ground for evolving criminal methodologies,⁹ making it increasingly affected by digital and AI-enabled crimes. As synthetic media-related crimes rise and legal frameworks in Southeast Asia remain in early stages, it is essential to support law enforcement in developing capacity to address these emerging threats.

In June 2024, INTERPOL launched a background paper titled [Beyond Illusions: Unmasking the Threat of Synthetic Media for Law Enforcement](#)¹⁰ in order to help law enforcement develop an introductory understanding of synthetic media and tackle the threats posed by this technology. Building on the foundation laid by this exploratory endeavour, in 2025 INTERPOL launched [Project SynthWave](#), which aims to support law enforcement in Southeast Asia in developing capabilities to detect AI-generated synthetic media and address related threats through community building, knowledge sharing, and regional collaboration.¹¹

This study, developed under Project SynthWave, endeavours to explore the growing challenges posed by synthetic media in Southeast Asia, while highlighting law enforcement response, use cases, and key recommendations to aid law enforcement in effectively preventing and combatting the threats posed by this technology. While the study adopts a regional focus on Southeast Asia, it should be noted that insights from this region can offer valuable guidance to law enforcement agencies globally as they prepare to confront similar challenges related to synthetic media.

1.1. Methodology

This study employed a qualitative research approach, with data collected through semi-structured interviews, virtual consultations, in-person member country visits, in-person events, and written questionnaires. The research for this study commenced during the Strategic Meeting for Project SynthWave, which was hosted by INTERPOL in April 2025. Over the course of the year, INTERPOL engaged with law enforcement experts from member countries in Southeast Asia to collect primary data. The study also draws on insights contributed by experts from industry, academia, and open-source research.

The primary data collected for the study were analysed to identify the most recurrent synthetic media threats in Southeast Asia, based on law enforcement experience. The information presented in the sections on law enforcement response including tools, reporting systems and awareness campaigns, and competence enhancement was acquired through the insights of law enforcement officers in the region,

complemented by open-source research. The recommendations put forth in this study were developed based on challenges and gaps identified through discussions with experts from law enforcement, industry, and academia. The main findings of this study were presented during the INTERPOL Conference on AI in Digital Forensics: Unpacking Insights in Investigations and Analysis which took place in October 2025 in Tokyo, Japan. Insights from this conference were incorporated in this study to reflect the latest developments in the area of synthetic media threats in Southeast Asia.

2. SYNTHETIC MEDIA THREATS IN SOUTHEAST ASIA

In 2024, the global prevalence of deepfakes rose by 245 per cent, accounting for 7 per cent of all fraud attempts.¹² Southeast Asia in particular has experienced a marked increase in the misuse of AI.¹³ Notably, four of the ten countries with the highest incidence of deepfake-related fraud are located in the region, with Singapore and Cambodia reporting the second-largest increase in such cases in 2024.¹⁴

The proliferation of synthetic media has not only contributed to the creation of new threats (such as using AI to write malicious code), but also led to the exacerbation of pre-existing threats with technologically evolved modus operandi. For example, according to an INTERPOL Crime Trend Update on Human Trafficking-Fueled Scam Centres, scam centres are being used for human trafficking and online financial fraud.¹⁵ AI techniques are being exploited to create job scams to lure human trafficking victims who are then forced to commit sextortion and romance scams, among other social engineering schemes.¹⁶

In Southeast Asia, the trend of using synthetic media to commit crimes has experienced a significant uptake recently, as it became a pressing concern for law enforcement in 2020 in Singapore, in 2022 in the Philippines, and in 2024 in Cambodia.¹⁷ In Southeast Asia, synthetic media crimes have manifested in various forms including **synthetic identities for digital fraud, non-consensual pornography, fabricating disinformation, and creating and disseminating malware at scale.**



Figure 2: Prominent synthetic media threats in Southeast Asia

For the purpose of this study, these crime trends have been placed under separate categories; however, it should be noted that they frequently intersect, creating a multiplier effect. Synthetic media can be misused to enable several criminal activities at once. For instance, AI-generated videos and images of public figures may constitute impersonation, while concurrently being used to spread political disinformation in order to cause societal unrest.

- **Synthetic identities for digital fraud:**
This crime refers to using AI-generated audio, video, and images to impersonate real individuals, steal real identities, and fabricate synthetic identities of individuals who do not exist. This identity theft and fraud identity generation can be used as means for various criminal ends.

- **Impersonation:** Synthetic media-enabled impersonation scams can be highly personalized to target specific individuals. Since the scams are specifically designed to entrap some individuals, their success rate can be higher. Impersonation and identity theft for financial fraud has emerged as a recurrent synthetic media crime threat for law enforcement in Southeast Asia. There have been multiple cases in the region where deepfake techniques were used to perpetrate elaborate, realistic scams for financial gain. In 2025, the Singapore Police Force and Hong Kong Police Force helped recover more than USD 499,000 after an employee of a multinational company was scammed into making the payment, in a case where the criminals used deepfake technology to impersonate the company's chief executive officer (CEO) and lawyer.¹⁸ According to the Global Anti Scam Alliance's (GASA) State of Scams in Southeast Asia 2025 Report, 63 per cent of the Southeast Asian adults surveyed claimed to have had a scam experience in the last 12 months, with investment, unexpected money, and impersonation scams being the most common.¹⁹ While not all criminals use synthetic media, the scam experience is made highly believable through the use of deepfakes, increasing the success rate of the scamming attempts.
- **Impersonation of public figures:** Within impersonation, the impersonation of public figures casts a wider net for scam victims. There have been a significant number of cases in Southeast Asia where deepfakes of public figures such as politicians, celebrities, and prominent business personalities have been used to commit financial scams. Law enforcement in countries in Southeast Asia has highlighted this trend as a critical synthetic media threat in the region. For instance, in 2024, the former Prime Minister of Singapore Lee Hsien Loong warned the public against a deepfake video of him promoting an investment scheme which was being circulated.²⁰ This incident came only a few months after a deepfake of him endorsing a cryptocurrency scheme had surfaced.²¹ Other countries in Southeast Asia have also been grappling with this rampant issue. In 2025, a deepfake video of Indonesian President Prabowo Subianto was circulated in a criminal attempt to scam victims into making payments across 20 provinces.²² Furthermore, in the Philippines, the Security and Exchange Commission (SEC) warned against a deepfake video of a prominent businessman which was being used to promote fraud cryptocurrency and forex schemes.²³ Since public figures and enterprises are highly credible, with the government being the most trusted institution in some countries in Southeast Asia,²⁴ such impersonation scams capitalize on their legitimacy. These scams can diminish public trust and contribute to the destabilization of societies.
- **Know-your-customer (KYC) scams:** These scams target institutions that are obliged to conduct KYC procedures, as criminals use deepfake technology to bypass their verification processes. KYC is a process used by financial institutions to verify a customer's identity before allowing them to open a bank account or make large transactions in order to prevent money laundering, tax evasion, terrorism financing, and other forms of financial crime. Criminals can bypass this online verification process by stealing identities of real people and/or fabricating synthetic identities which can be used to complete the verification process, including passing liveness checks. For instance, Vietnamese authorities recently dismantled a criminal ring that laundered an estimated USD 39 million over a seven-month period by circumventing banking protocols through the use of AI-generated synthetic identities²⁵.
- **Romance scams:** One of the most widespread impersonation scams in Southeast Asia is the romance scam, in which fraudsters assume real or fabricated identities to deceive vulnerable victims by feigning romantic interest. Increasingly, these schemes employ

synthetic media to enhance realism and scale. In a recent case, a criminal ring stole USD 46 million by committing deepfake-based romance scams that targeted men across several Asian countries.²⁶ Beyond video and audio deepfakes, scammers can also use synthetic tools to generate and translate scripts, making interactions more personalized and contextual. They can also deploy deepfake bots that create and sustain entire personas with minimal human oversight, enabling such scams to be conducted at scale.²⁷

- **Non-consensual pornography:**

- **Sextortion:** Sextortion refers to a form of online blackmail where criminals threaten to share sexual pictures, videos, or information about the victim to extort money or other favours from them. This crime type has been exacerbated through the use of deepfakes as criminals can create fake images and videos that are sexually explicit. Sextortion has emerged as another prominent crime threat for law enforcement in Southeast Asia. In a mass sextortion attempt in November 2024, more than 100 public servants across more than 30 government agencies in Singapore received sextortion threats demanding USD 50,000 each to not release their images which had been doctored to appear sexually explicit.²⁸ Advances in synthetic media technology have made the creation of sexually explicit content increasingly accessible, enabling the use of any and every individual's likeness for such purposes. This technology also facilitates large-scale exploitation, as a single piece of content can be reused to extort multiple victims by simply substituting faces. While the term sextortion typically refers to cases in which perpetrators seek monetary or other tangible favours from the victims in exchange for not releasing the content, sexually explicit fabricated imagery may also be used as a means of harassment, bullying, or defamation. The lack of technical skills and equipment needed to create such content has lowered the barrier for producing such content, making it accessible to a wide range of criminals. Furthermore, victims of these "virtual assaults" suffer extreme emotional and psychological trauma due to this digital harassment and defamation. For instance, in Indonesia, a university student was accused of stealing photos of his female peers from social media and creating sexually explicit deepfakes, causing "emotional distress and trauma to at least 37 individuals."²⁹ Therefore, the use of synthetic media technology to create and weaponize sexually explicit deepfakes is a recurrent issue in Southeast Asia.
- **Child sexual abuse material (CSAM):** Synthetic media are also being misused to create sexually explicit deepfakes of minors. The Internet Watch Foundation (IWF) assessed more than 8,029 AI-generated images and videos depicting realistic child sexual abuse across the dark web and the clear web in 2025. Its analysis found that realistic AI-generated child sexual abuse videos have become increasingly prevalent, with 65% of the videos assessed classified as Category A - the most severe classification³⁰. The use of synthetic media to create CSAM in Southeast Asia has also been highlighted as a growing concern by law enforcement. Since the generation of such material no longer requires technical expertise or sophisticated software and equipment, the opportunity and ability to create such material has magnified. School students in Singapore in 2024 were accused of creating sexually explicit deepfakes of their female peers.³¹ A few months later, in Malaysia in April 2025, a teenage boy was accused of creating and selling explicit deepfakes of his female schoolmates on social media platforms.³² Therefore, the evolution of synthetic media technology has empowered not only highly organized, technically sophisticated criminal groups operating on the dark web, but also

non-technical individuals who can now create CSAM with minimal skill and readily available equipment.

- **Disinformation:**

Disinformation can be understood as false information that is disseminated intentionally to cause serious social harm.³³ While synthetic-media-enabled audio, video, and images can be used to perpetrate disinformation among other crimes, one of the main sources of disinformation is AI-generated text. Focusing on the “social harm” aspect of this malicious activity, disinformation during elections, which can debilitate public safety, has emerged as a pressing concern for law enforcement in Southeast Asia. Sumsu, which is an identity verification platform, reported that 85 per cent of the respondents surveyed in Asia Pacific (APAC) expressed fear about the impact of deepfakes on present and future elections.³⁴

Ahead of the 2024 regional elections in Indonesia, the government revealed the takedown of “probably thousands” of deepfake accounts and content which could cause division in society.³⁵ Similarly, ahead of the 2025 mid-term elections in the Philippines, the government warned of deepfakes and cyberattacks becoming more rampant.³⁶ Furthermore, generative AI can be used to enhance website spoofing efforts, from creating design and logos that mimic authentic websites to producing massive amounts of content and articles to populate the website. These websites can be used to not only scam individuals by tricking them into following malicious links, but they can also be used to create disinformation against the legitimate authorities that they aim to impersonate. In October 2024, the Singapore Ministry of Home Affairs identified 10 inauthentic websites which were allegedly established to spread hostile information campaigns.³⁷

- **Creating and disseminating malware at scale:**

Synthetic media technology can be used to create and deploy fraud schemes; however, it can also be used to create malicious actors which can perpetrate harmful activities at scale with little human intervention. Criminals can use synthetic media for the mass creation of bots which can be designed to perpetrate an array of crimes such as disinformation, scams, and phishing. Generative AI can also be used to write malicious code, which would not only expedite the rate at which criminals can create malware but also allow non-technical experts to engage in such activities with ease.³⁸ While examples of criminals misusing this technology in Southeast Asia are not rampant, it has been highlighted by law enforcement as an emerging trend with implications for future policing.

Therefore, the most recurrent synthetic media threats in law enforcement include: synthetic identities for digital fraud, and scam variants such as KYC and romance scams; non-consensual pornography through sextortion and the creation and dissemination of CSAM; fabricating disinformation to cause societal harm and unrest; and creating and disseminating malware at scale. Based on consultations and interviews conducted with member countries, the most frequently mentioned threats were: impersonation of public figures; impersonation of civilians; identity fraud and deepfake pornography; fake news, fake news during elections, and online harassment; and other crimes such as forgery, voice phishing, website spoofing, and defamation, in the indicated order.

Despite the rise in synthetic media crime in Southeast Asia, the number of reported cases remain low relative to the perceived scale of the threat, with Laos recording no synthetic media cases in the past year, Cambodia reporting only three cases, and the Philippines reporting seven cases out

of the 10,004 cybercrime cases registered.³⁹ Several factors may explain the discrepancy between trends and recorded statistics. For instance, there is no distinct classification of AI or synthetic-media-related offences, which are often subsumed under broader categories such as cybercrime or reported in terms of their resulting harms (e.g. identity theft, child abuse, defamation). Frameworks for AI taxonomy are needed to enable more accurate classification of synthetic media and AI-related crimes, supporting effective reporting, improving threat visibility, and allowing law enforcement to allocate resources more efficiently. Given the transnational nature of synthetic media and AI crimes, there is a need to establish a common regional and international understanding of AI taxonomy to enable seamless law enforcement collaboration across jurisdictions. Moreover, limited public awareness of synthetic media technologies means that victims may not even recognize that they have been targeted by such crimes. Additionally, gaps in law enforcement understanding of these technologies also hinder their ability to guide citizens and effectively register complaints. Consequently, there is a need to raise awareness of synthetic media crimes and their implications among both the public and all levels of law enforcement, particularly frontline officers who interact directly with citizens.

3. LAW ENFORCEMENT RESPONSE TO SYNTHETIC MEDIA THREATS

Amid evolving synthetic media threats, law enforcement is ramping up response to such crimes by actively acquiring cutting-edge tools, leveraging digital reporting systems, deploying awareness campaigns, engaging in competence-enhancement efforts, and forging multisectoral partnerships with subject-matter experts.

3.1.Tools⁴⁰

Due to lack of resources, law enforcement agencies are not always able to acquire latest deepfake detection tools or build them in-house. Consequently, some law enforcement agencies must rely on open-source tools which are not very accurate or efficient to use. Nonetheless, law enforcement in Southeast Asia has been working with private-sector partners to acquire deepfake detection tools while some agencies have been able to build their own tools with the help of in-house specialists.

For audio forensics, the Royal Malaysian Police Force relies on an externally acquired deepfake detection tool which conducts speaker verification, detects audio spoofing, and can be deployed on site and through private clouds so that sensitive data do not leave the server. In the Philippines on the other hand, the Cybercrime Investigation and Coordination Center (CICC)⁴¹ conducts deepfake detection with the help of an acquired tool which can detect a deepfake video in 30 seconds.

While most countries have acquired deepfake detection tools or use open-source tools, the Singapore Police Force (SPF) uses a combination of externally acquired and in-house tools which apply a series of algorithms to detect altered or synthetically generated content.

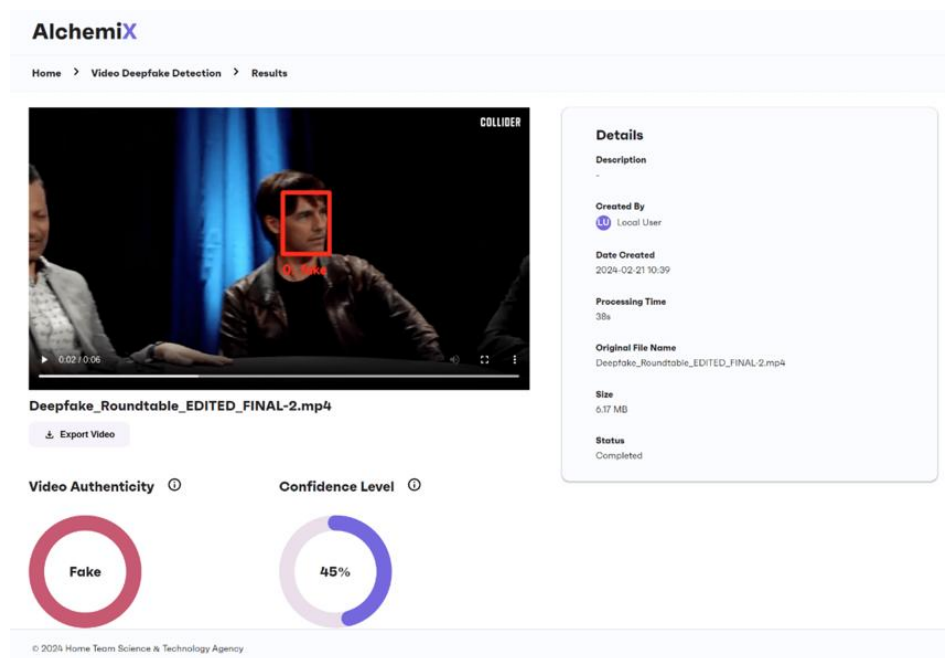


Figure 3: Deepfake detection tool AlchemiX, developed by HTX, Singapore

Source : [HTX, Singapore](#)

For image, audio, and video forensics, SPF uses an internally developed digital forensics tool in combination with another in-house tool named AlchemiX⁴² (Figure 3), developed by Singapore's Home Team Science and Technology Agency (HTX), and a third externally acquired audio, video, and image deepfake detection tool which can work in real-time and be deployed on site or through the cloud to secure sensitive data.

The agency uses another acquired deepfake detection platform specifically for cloud-based detection which can process videos, images, audio, and virtual identities. For deeper analysis, SPF wields further tools that:

- detect inconsistencies and conduct device identification through sensor analysis, metadata inspection, and examination of the file structure and properties.
- verify media for traces of modification, tracking metadata inconsistencies and tracing the history of file edits.
- conduct deepfake audio detection which can be run on site within a Windows desktop application for audio extraction (from video), conversion, and playback. This version allows users to control the selection of detection models and configure Red Amber Green (RAG) decision thresholds. The same detection models can also be on the web version, which allows multiple analysts to provide their samples collaboratively.

In their efforts to acquire, develop, and utilize deepfake detection tools, law enforcement agencies face significant challenges such as budgetary restrictions and difficulties in post-detection attribution.

3.2. Reporting systems and awareness campaigns

The first step towards response comes from creating dedicated reporting systems where citizens are encouraged to register crimes and suspicious activities. Since synthetic media content is perpetrated digitally, online reporting systems have been leveraged by law enforcement to register synthetic media cases. Law enforcement in Viet Nam leverages the VNeID platform, which is a digital identity platform where the public can also report crimes, including synthetic media crime. The Philippines uses an Inter-Agency Response Center Hotline (1326) to centralize the reporting of online scams, including synthetic media scams.⁴³ Most law enforcement agencies also use their social media accounts to raise public awareness about AI-enabled threats, which often leads to members of the public submitting complaints directly through these platforms.

While tools and reporting systems contribute to the retroactive response towards synthetic media crimes, government agencies, law enforcement authorities, and financial institutions are also adopting a proactive approach to preventing these crimes through public awareness campaigns.

Following a misuse of its name and logo, the Brunei Darussalam Central Bank (BDCB) issued a press release warning the public against AI-generated fake news items which use clickbait headlines to trick customers into revealing sensitive information and infect their devices with malware. In the advisory, the BDCB shared best practices to safeguard against such AI-enabled threats such as verifying sources and reporting suspicious content.⁴⁴ Given the vulnerability of the financial sector against AI-enabled deepfake crime and investment frauds, Bank Central Asia (BCA) Indonesia also released an article urging customers to be wary of deepfake scams while providing security tips on how they could protect themselves against such scams.⁴⁵

In Indonesia, the Deputy Minister of Communication and Digital Affairs issued a statement asking people to remain vigilant against AI-enabled fraud, especially deepfake scams. The Minister specifically advised vigilance against new types of financial scams being undertaken with the use of synthetic media.⁴⁶ Furthermore, the government issued a regulatory letter to business actors in the public and private sector on the ethical use of AI to combat deepfake crimes. The letter also encouraged technology providers including social media platforms to identify and remove harmful AI-generated content.⁴⁷

Law enforcement agencies across the region actively disseminate information on popular deepfake scams to create public awareness and enhance citizen preparedness against specific modus operandi being used by criminals. In Malaysia, the Commercial Crime Investigation Department (CCID) warned the public against deepfake-enabled investment scams misusing the likeness of international and local public figures, politicians, and business personalities.⁴⁸ In the past, the CCID has also urged the public to come forward and register reports if they have been victimized by deepfake crime, highlighting the importance of authentication by the victim to respond to such crimes.⁴⁹ Similarly, in 2022, the Thai police disseminated information on an ongoing scam being perpetrated by “call centre” gangs who were exploiting publicly available footage of law enforcement officers to create deepfakes and trick victims into believing that they were receiving a video call from the police.⁵⁰ In December 2023, the Thai police also warned the public of an impending surge of synthetic media crime and deepfake scams in 2024, especially for the perpetration of non-consensual pornography, AI-generated disinformation, and financial scams.⁵¹ Such statements heighten vigilance and awareness among citizens regarding the most common types of threats and criminal modus operandi related to this new technology.



Figure 4: Advisory on the CICC’s website against deepfake phishing

Source: [CICC’s website](https://cicc.gov.ph)

Law enforcement and government agencies also often provide public awareness information periodically through their websites, social media channels, and physical visits to public sites. Since Facebook is the primary social media platform used in the Philippines, apart from using its website⁵² (Figure 4), the Cybercrime Investigation and Coordination Center (CICC) leverages its Facebook page to disseminate information regarding deepfake crimes and debunk viral deepfake content which is aimed at defrauding citizens.⁵³ The CICC’s Facebook page also sees significant activity related to citizens reporting deepfake crime.⁵⁴ Apart from digital awareness campaigns, the Philippine National Police (PNP) also conduct Barangay visitations to undertake physical outreach and create awareness regarding new types of crimes. Barangay visitation refers to local government and law enforcement entities visiting villages to provide essential services and information for public wellness and safety.

Singapore’s government agencies and law enforcement have launched extensive collaborative and multifaceted initiatives to create public awareness regarding digital scams, which also covers synthetic media scams. SPF, the Monetary Authority of Singapore (MAS) and the Cyber Security Agency of Singapore (CSA) issued a joint

advisory against a synthetic media scam variant wherein criminals were impersonating high-ranking executives from companies to dupe employees of the company into transferring company funds. The advisory also suggested precautionary measures for businesses to safeguard themselves and their employees against such scams.⁵⁵ In 2023, the Singapore government launched the “I can ACT against scams” campaign to create awareness against various types of scams, including synthetic media scams. The campaign propagates “Act, Check, Tell” (ACT) as a framework to respond to scams.⁵⁶ The CSA also released an advisory outlining the 3A approach on how to detect deepfakes (Figure 5). The three-pronged approach includes the following steps: “Assess the message, Analyse audiovisual contents, and Authenticate content using tools.”⁵⁷ This approach falls under the “Check” component of the ACT framework against scams.

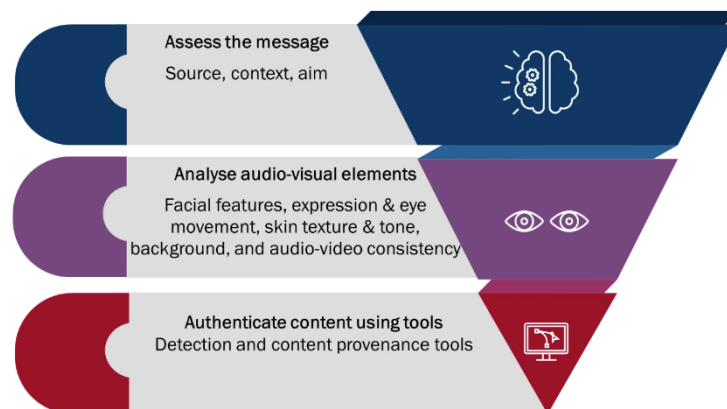


Figure 5: The 3A approach for detecting deepfakes created by the Cyber Security Agency (CSA) of Singapore

Source: [CSA, Singapore](#)

The government has also introduced ScamShield, which consists of a helpline, an app, and a website to provide tools and resources for scam prevention.⁵⁸ Other initiatives include displaying posters in public spaces such as the Mass Rapid Transit (MRT) stations to raise awareness against scams, including synthetic media scams.⁵⁹



Figure 6: Impersonation scam awareness poster created by ScamShield, Singapore.

Source: [ScamShield, Singapore](#)

3.3. Competence enhancement

In order to effectively respond to synthetic media threats, law enforcement must be equipped with the knowledge and ability to detect, investigate, and attribute related content. While some law enforcement agencies in Southeast Asia offer such learning opportunities to their officers, most agencies remain in the early stages of these competence enhancement efforts and provide overarching guidance on digital transformation within which AI and synthetic media may be a component.

The Philippine Public Safety College houses the National Cyber Training Institute which collaborates with academia to provide training for officers on AI, among other subjects. Commissioned officers receive specialized guidance, while non-commissioned officers receive basic guidance during which they are taught to create and detect synthetic media. Learning opportunities are also provided to on-the-ground officers who are more likely to interact with civilians. With the aim of expanding the concept of law enforcement, learning opportunities are not just limited to officers in the PNP, but also officers in the bureau of immigration, coastguard, jail management, and other agencies.⁶⁰

In Singapore, SPF offers learning opportunities and a pool of resources in order to build officers' capabilities in investigating synthetic media cases. Specialists participate in advanced courses, some of which are delivered by industry partners. Within the Technology Crime Forensics Branch (TCFB), officers participate in foundational levels of evidence-based forensic video and digital multimedia evidence processing courses and officers investigating multimedia cases receive the advanced version of this course. Upon meeting certain requirements, officers are also able to train further in audio and forensic imaging techniques. Furthermore, HTX developed an AI learning roadmap to empower officers across law enforcement in Singapore to use AI tools effectively.⁶¹

Furthermore, the role of partnerships is crucial in preventing and combatting the criminal misuse of any emerging technology. As law enforcement attempts to keep pace with increasingly sophisticated criminal actors, it is imperative to leverage the expertise of industry and academic partners, who possess the latest knowledge and tools to support law enforcement efforts. Apart from the acquisition of tools, it is also important for law enforcement to collaborate with technology providers and social media companies for the effective identification and takedown of harmful synthetic media content on their platforms.

Amid deepfakes and political disinformation threatening to hamper the integrity of elections, Indonesian political parties and candidates agreed to comply with a voluntary social media usage framework during campaigning.⁶² Such coalitions for self-regulation are a step towards promoting the ethical use of AI while responding to the misuse of synthetic media to perpetrate societal harms. In the Philippines, the Commission on Elections (Comelec) convened multiple stakeholders including government agencies, social media platforms, and civil society groups to form a task force to combat AI-generated disinformation during elections and maintain the integrity of the polls.⁶³ This includes real-time monitoring of election-related cyber activity ranging from disinformation networks to potential cyberattacks, using tools designed for early detection and swift action.

The lack of a common understanding and standardized policies on what is considered harmful creates a challenge for law enforcement in cooperating with private industry whose responses to different types of media can be different. While some social media platforms proactively respond to law enforcement's request to block and remove most harmful content, some platforms may only block certain explicit

content, while others may not block any content at all. Therefore, law enforcement response to such instances tends to take on a case-by-case approach based on the partners involved.

While collaboration with private sector, academia, and civil society is significant, it is also crucial for law enforcement to undertake interagency, regional, and international cooperation to not only combat synthetic media crime itself, but also disrupt other aspects of the crime lifecycle. For instance, as mentioned in Section 2 of this study, in the 2025 case where an employee was duped into making a large payment by criminals who used synthetic media to impersonate the company's CEO, Singapore Police Force's Anti-Scam Centre (ASC) and Hong Kong Police's Anti-Deception Coordination Centre (ADCC) worked together to recover USD 499,000 by thwarting the bank transfer. Given that the location of the laundered proceeds was different from the location where the scam was committed, ASC and ADCC's swift and collaborative response to this crime helped with the recovery. Additionally, the ASC also seized the remaining money in the local mule account, disrupting the money flow.⁶⁴ Given the borderless nature of synthetic media crime, victims and perpetrators may be spread across countries and regions. Therefore, international and regional law enforcement cooperation is imperative in identifying and capturing criminals misusing synthetic media to perpetrate harms. For instance, in 2025, in a cross-agency collaborative operation, officers from the Singapore Police Force, Hong Kong Police Force, National Police Agency of Japan, Korean National Police Agency, Royal Malaysia Police, and Royal Thai Police arrested 435 criminals engaged in online child sexual exploitation activities which included AI-generated CSAM.⁶⁵ With victims and perpetrators based across various countries, this collaborative approach targeting child abuse resulted in comprehensive action. Collaborative takedowns can achieve greater scale when dealing with transnational crimes such as AI crimes, as opposed to actions undertaken in individual jurisdictions.

While regional collaboration on combatting synthetic media threats exists in areas such as financial crime and combating CSAM where synthetic media are often a component, the growing criminal use of AI and synthetic media highlights the need for more coordinated cooperation. Convening experts currently dispersed across different crime areas and regions would facilitate the exchange of best practices and insights on the criminal exploitation of this technology across crime types.

4. RECOMMENDATIONS

- **Competency enhancement:** Responding to the criminal use of emerging technologies like synthetic media requires extensive skills development and competence enhancement for law enforcement. While some law enforcement agencies offer learning opportunities related to audiovisual forensics, most agencies are unable to engage in these capability-enhancement efforts due to lack of resources and expertise. All law enforcement officers should undergo foundational learning to help them understand AI and synthetic media crimes so that they are able to effectively support victims and encourage them to report such cases. Moreover, officers working in the area of multimedia, forensics, and cybercrime should be upskilled further to allow them to detect, trace, and attribute deepfakes and synthetic media content. Additionally, it is crucial for other actors in the criminal justice system to have fundamental understanding of synthetic media in order to effectively prosecute such cases. Judges and prosecutors should receive foundational guidance on how such material is created and investigated to support their understanding of the evidence and the chain of custody process when such cases are submitted to the court.⁶⁶
- **Guidelines:** Given the evolving nature of synthetic media crimes, there is a need for updated regulations and guidelines on how to categorize and respond to these crimes. A clear understanding on the classification of AI-generated material based on the degree of harm – coupled with clear protocols on how to respond to each degree of harm – should be established, as this would not only allow law enforcement to undertake swift and proportionate action across agencies, but also cooperate with private partners for effective takedowns. Furthermore, the guidelines should not only cover the protocols for takedown, but also address various stages in the entire lifecycle of crime, providing an end-to-end approach towards response. For instance, in a case of money laundering through deepfake-enabled financial scams, guidelines should also address how to disrupt the flow of money and mule accounts. Additionally, uncertainties surrounding the admissibility of AI-based forensic findings in court hamper law enforcement's ability to conduct synthetic media investigations. Since most detection tools rely on AI, there is a need for clear procedural guidance on how such evidence can be documented, validated, and effectively presented in judicial proceedings.
- **Partnerships:** Synthetic media crime is digital and complex in nature, making it difficult for law enforcement to disrupt with traditional methods. Therefore, there exists a need for multiple levels of partnerships to effectively prevent and disrupt such crime. As described in the previous sub-sections, law enforcement agencies across Southeast Asia have undertaken several partnerships with the private sector and academia for the acquisition of tools, creation of learning opportunities, etc. However, there is a need to significantly enhance these partnerships, turning them into a pillar of law enforcement's response to synthetic media threats.
 - **Private sector:** Partnerships with the private sector are crucial for several aspects of law enforcement response including detection, investigation, and takedown. Law enforcement should leverage the expertise of private sector partners to attain access to or collaboratively build detection tools, which can help them

identify and trace synthetic media contents effectively. Furthermore, since harmful synthetic media content is disseminated or exchanged through online forums, robust cooperation with social media platforms and technology providers is also required for immediate takedowns and action. Clear protocols and memoranda of understanding should be forged between law enforcement and social media platforms to ensure swift and standardized action.

- **Expert groups:** Additionally, in order to expand law enforcement's knowledge and understanding of this dynamic technology, multisectoral expert groups should be created consisting of law enforcement, digital forensic experts, social media platforms, and researchers so that the latest information on the criminal use of synthetic media, including new modes of misuse, can be shared and timely response mechanisms can be created. Such groups can also serve as threat assessment hubs which identify and classify emerging threats, while disseminating knowledge on prevention and detection methodologies. Leveraging its networks of global experts, INTERPOL can act as the convenor of such expert groups.
- **Interagency regional and global collaboration:** Given the transnational nature of such crimes, it is crucial for law enforcement to undertake interagency collaboration regionally and globally. There is a strong imperative for law enforcement to undertake cooperative efforts including not only joint action for takedowns, but also the sharing of best practices. Due to the sensitive nature of such crimes, agencies are often reluctant to share information. Secure information exchange can be achieved through INTERPOL channels which offer a safe global communications system.

5. ROLE OF INTERPOL

As the international organization facilitating global law enforcement cooperation, INTERPOL's role is critical in helping the law enforcement community stay ahead of rapidly evolving criminal threats by fostering meaningful collaboration, undertaking capability-enhancement efforts, raising awareness, and facilitating knowledge sharing.

Having identified synthetic media as an emerging technology with implications for the crime landscape and law enforcement, INTERPOL endeavours to raise awareness regarding this subject. Building on the foundation of the 2024 background paper titled [Beyond Illusions: Unmasking the Threat of Synthetic Media](#),⁶⁷ INTERPOL launched [Project SynthWave](#)⁶⁸ in 2025, which aims to assist law enforcement in building capabilities to detect AI-generated synthetic media and counter the threats posed by this technology. While the project focuses on Southeast Asia to foster regional collaboration, the learnings from the project have global implications as the misuse of synthetic media continues to evolve as an international concern. Through such projects, INTERPOL can promote community building, knowledge sharing, and regional collaboration to help law enforcement combat the threats associated with this technology.

Leveraging its crime trend knowledge, INTERPOL can continue disseminating awareness regarding various crime modalities which misuse synthetic media technology, such as human trafficking-fuelled scam centres exploiting AI to transform scams.⁶⁹ Furthermore, INTERPOL can also publish notices to share information on synthetic media misuse. INTERPOL notices are international requests for cooperation or alerts allowing police in member countries to share critical crime-related information. The INTERPOL purple notice in particular is issued to seek or provide information on modus operandi, objects, devices, and concealment methods used by criminals.⁷⁰ INTERPOL can issue purple notices to disseminate further information on new criminal modus operandi using synthetic media. This would also underscore the significance and pervasiveness of the misuse of synthetic media technology to commit crimes. Additionally, as mentioned in the previous section, INTERPOL can leverage its robust networks of law enforcement experts, digital forensic experts, social media platforms, and researchers to create multisectoral expert groups for cross-sharing of the latest information on synthetic media threats and co-creation of response mechanisms. Lastly, given the sensitive nature of synthetic media crime, law enforcement agencies are often apprehensive of exchanging intelligence and best practices. To share such information, member countries can leverage INTERPOL's secure global communications system, i24/7, which is the technical network that links law enforcement in all member countries and enables authorized users to share sensitive and urgent police information with their counterparts around the globe.⁷¹

Therefore, INTERPOL can enhance law enforcement's capabilities in navigating synthetic media crime by providing its tools and services, facilitating meaningful partnerships between law enforcement, industry and academia, and undertaking capability enhancement and knowledge-sharing efforts.

6. CONCLUSION

With the growing criminal exploitation of synthetic media exacerbating existing offences and enabling new ones, law enforcement and government agencies are grappling with a rapidly evolving threat landscape. As synthetic media technology continues to evolve, this threat landscape will become even more complex, warranting a multifaceted response. While some Southeast Asian countries have introduced dedicated frameworks to address synthetic media harms, many responses remain fragmented and inconsistent. Limited regional coordination and uneven awareness of synthetic media threats could further hinder law enforcement's ability to respond to such crime. Therefore, the development of a taxonomy to classify AI-related crimes could support law enforcement in identifying pathways to establish collaboration.

Law enforcement agencies are responding to the misuse of this technology on multiple fronts by developing tools, raising public awareness, undertaking competence-enhancement efforts, and building partnerships. However, as synthetic media evolves in sophistication and scale, these efforts – which are currently in nascent stages – need to be significantly amplified. Strengthening partnerships with the private sector and academia is key, not only to jointly create and acquire detection tools, but also to develop updated and forward-looking learning opportunities to equip law enforcement and criminal justice actors with appropriate expertise to investigate synthetic media content and adequately handle such cases in court. Furthermore, given the borderless nature of synthetic media crimes, victims and perpetrators are located across regions and jurisdictions, making cross-border regional and international law enforcement cooperation indispensable. Joint takedown efforts, regular information-sharing, and the exchange of best practices should be further promoted to allow law enforcement agencies to build on each other's experiences and avoid duplication of effort.

Building resilience against synthetic media threats in Southeast Asia warrants a holistic approach that not only strengthens current efforts, but also prepares for the evolving threat landscape by leveraging partnerships and enhancing regional and global law enforcement cooperation. As the organization facilitating regional and global law enforcement cooperation, INTERPOL has a key role to play in connecting experts, disseminating knowledge, and promoting thought leadership on how to prevent and combat synthetic media crime. While this study focuses on Southeast Asia, the experiences and insights from this region can also offer valuable guidance to the international law enforcement community as it prepares to prevent and combat similar threats. In the future, INTERPOL also aims to explore global insights on synthetic media threats and law enforcement response to facilitate the exchange of global best practice

REFERENCES

- ¹ INTERPOL, *Beyond Illusions: Unmasking the Threat of Synthetic Media for Law Enforcement*, June 2024, <https://www.interpol.int/en/How-we-work/Innovation/INTERPOL-Innovation-Centre>, last accessed 5 January 2026.
- ² Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 on laying down harmonized rules on artificial Intelligence (Artificial Intelligence Act) and amending certain Union legislative acts, *Official Journal of the European Union*, L 157, 14 June 2024, art. 3, <https://artificialintelligenceact.eu/article/3/>, last accessed 5 January 2026.
- ³ European Parliament and the Council of the European Union, 2024.
- ⁴ MIT Sloan School of Management, *Deepfakes, explained*, July 2020, <https://mitsloan.mit.edu/ideas-made-to-matter/deepfakes-explained>, last accessed 5 January 2026.
- ⁵ Greater Manchester Police, *Man who created indecent images using AI-enabled technology sentenced to 24 years*, October 2024, <https://www.gmp.police.uk/news/greater-manchester/news/news/2024/october/man-who-created-indecent-images-using-ai-enabled-technology-sentenced-to-24-years/>, last accessed 5 January 2026.
- ⁶ Bobby Chesney and Danielle Citron, *Deep Fakes: A Looming Challenge for Privacy, Democracy, and National Security*, December 2019, <https://www.californialawreview.org/print/deep-fakes-a-looming-challenge-for-privacy-democracy-and-national-security>, last accessed 5 January 2026.
- ⁷ Dorna Moini, *AI on trial: How courts are litigating the GenAI boom*, November 2024, <https://www.thomsonreuters.com/en-us/posts/ai-in-courts/courts-genai-boom/>, last accessed 5 January 2026.
- ⁸ Google, Temasek, and Bain, *e-Conomy SEA 2023*, <https://www.temasek.com.sg/content/dam/temasek-corporate/news-and-views/resources/reports/google-temasek-bain-e-conomy-sea-2023-report.pdf>, last accessed 5 January 2026.
- ⁹ United Nations Office on Drugs and Crime, *Emerging threats: The intersection of criminal and technological innovation in the use of automation and artificial intelligence in the cybercrime landscape of Southeast Asia*, September 2025, https://www.unodc.org/roseap/uploads/documents/Publications/2025/UNODC_Report_Emerging_threats_-_The_intersection_of_criminal_and_technological_innovation_in_the_use_of_automation_and_AI.pdf, last accessed 5 January 2026.
- ¹⁰ INTERPOL, 2024.
- ¹¹ INTERPOL, *How we work, Innovation, Project SynthWave*, <https://www.interpol.int/en/How-we-work/Innovation/Projects/Project-SynthWave>, last accessed 5 January 2026.
- ¹² The Sumsuher, Expert-led anti-fraud media, *Identity Fraud Report 2024-2025*, January 2025, <https://sumsub.com/blog/guides-reports/identity-fraud-report-2024-2025/>, last accessed 5 January 2026.
- ¹³ United Nations Office on Drugs and Crime, *Transnational Organized Crime and the Convergence of Cyber-Enabled Fraud, Underground Banking and Technological Innovation in Southeast Asia: A Shifting Threat Landscape*, October 2024, https://www.unodc.org/roseap/uploads/documents/Publications/2024/TOC_Convergence_Report_2024.pdf, last accessed 5 January 2026.
- ¹⁴ The Sumsuher, Expert-led anti-fraud media, *Identity Fraud Report 2024-2025*, January 2025, <https://sumsub.com/blog/guides-reports/identity-fraud-report-2024-2025/>, last accessed 5 January 2026.
- ¹⁵ INTERPOL, News and Events, *INTERPOL Crime Trend Update, Human trafficking-fueled scam centres*, June 2025, <https://www.terpol.int/en/News-and-Events/News/2025/INTERPOL-releases-new-information-on-globalization-of-scam-centres>, last accessed 5 January 2026.
- ¹⁶ INTERPOL, 2024.
- ¹⁷ Source: INTERPOL virtual and in-person consultations with the Singapore Police Force, Philippines National Police, and Cambodian National Police.
- ¹⁸ The Straits Times, *Finance director nearly loses \$670k to scammers using deepfakes to pose as senior execs*, April 2025, <https://www.straitstimes.com/singapore/finance-director-nearly-loses-670k-to-scammers-using-deepfakes-to-pose-as-company-senior-execs>, last accessed 5 January 2026.

-
- ¹⁹ Global Anti-Scam Alliance (GASA), *State of Scams in Southeast Asia 2025 Report*, August 2025, <https://www.gasa.org/post/new-study-reveals-63-of-southeast-asians-experienced-scams-in-past-year>, last accessed 5 January 2026.
- ²⁰ The Straits Times, *SM Lee warns that video of him promoting investment scam on social media is a deepfake*, June 2024, <https://www.straitstimes.com/singapore/sm-lee-warns-that-video-of-him-promoting-an-investment-scam-on-social-media-is-a-deepfake>, last accessed 5 January 2026.
- ²¹ The Straits Times, *SM Lee warns that video of him promoting investment scam on social media is a deepfake*, June 2024, <https://www.straitstimes.com/singapore/sm-lee-warns-that-video-of-him-promoting-an-investment-scam-on-social-media-is-a-deepfake>, last accessed 5 January 2026.
- ²² The Straits Times, *Indonesians swindled by scams using President Prabowo deepfakes*, March 2025, <https://www.straitstimes.com/asia/se-asia/indonesians-swindled-by-scams-using-president-prabowo-deepfakes>, last accessed 5 January 2026.
- ²³ InsiderPH, *EC warns public: Deepfake scam uses tycoon Lance Gokongwei to push fake crypto deals*, July 2025, <https://insiderph.com/sec-warns-public-deepfake-scam-uses-tycoon-lance-gokongwei-to-push-fake-crypto-deals>, last accessed 5 January 2026.
- ²⁴ Channel News Asia, *Government remains most trusted institution in Singapore, amid global trend of societal polarisation: Survey*, March 2023, <https://www.channelnewsasia.com/singapore/edelman-trust-barometer-2023-government-business-polarisation-inequality-3345571>, last accessed 5 January 2026.
- ²⁵ VN Express International, *Vietnam police bust \$39M money laundering ring that used AI face scan*, May 2025, <https://www.vnexpress.net/news/vietnam-police-bust-39m-money-laundering-ring-that-used-ai-face-scans-4488888.html>, last accessed 5 January 2026.
- ²⁶ CCN World, *Deepfake romance scam raked in \$46 million from men across Asia, police say*, October 2024, <https://edition.cnn.com/2024/10/15/asia/hong-kong-deepfake-romance-scam-intl-hnk/index.html>, last accessed 5 January 2026.
- ²⁷ The Strait Times, *Scammers using AI to dupe the lonely looking for love, Meta warns*, February 2025, <https://www.straitstimes.com/world/scammers-using-ai-to-dupe-the-lonely-looking-for-love-meta-warns>, last accessed 5 January 2026.
- ²⁸ Channel News Asia, *Ministers among more than 100 Singapore public servants sent extortion notes with 'compromising' deepfake images*, November 2024, <https://www.channelnewsasia.com/singapore/over-100-government-staff-30-agencies-extortion-emails-fake-obscene-images-4775931>, last accessed 5 January 2026.
- ²⁹ Jakarta Globe.ID, *Bali's Udayana University Expels Student Over Deepfake Sexual Harassment Case*, May 2025, <https://jakartaglobe.id/tech/balis-udayana-university-expels-student-over-deepfake-sexual-harassment-case>, last accessed 5 January 2026.
- ³⁰ Internet Watch Foundation (IWF), *AI-Generated Child Sexual Abuse: 2026 Report on Trends, Data & Human Impact*, 2026, <https://www.iwf.org.uk/about-us/why-we-exist/our-research/how-ai-is-being-abused-to-create-child-sexual-abuse-imagery/>, last accessed 31 July 2026.
- ³¹ Channel News Asia, *Police investigating deepfake nude photos of Singapore Sports School students*, November 2024, <https://www.channelnewsasia.com/singapore/singapore-sports-school-deepfake-nude-images-students-police-investigating-4742506>, last accessed 5 January 2026.
- ³² The Online Citizen, *16-year-old student in Malaysia arrested for creating and selling lewd AI-generated deepfake of schoolmates*, April 2025, <https://www.theonlinecitizen.com/2025/04/10/16-year-old-student-in-malaysia-arrested-for-creating-and-selling-lewd-ai-generated-deepfake-of-schoolmates/>, last accessed 5 January 2026.
- ³³ United Nations General Assembly. (2022, August 12). *Countering disinformation for the promotion and protection of human rights and fundamental freedoms, Report of the Secretary-General [Resolution A/77/287]*, August 2022, <https://docs.un.org/en/A/77/287>, last accessed 5 January 2026.
- ³⁴ The Sumsuher Expert-led anti-fraud media, *Identity Fraud Report 2024-2025*, January 2025, <https://sumsub.com/blog/guides-reports/identity-fraud-report-2024-2025/>, last accessed 5 January 2026.
- ³⁵ Tempo English, *Indonesian Govt Takes Down Thousands of Deepfake Accounts, Contents ahead of Regional Elections*, September 2024, <https://en.tempo.co/read/1915950/indonesian-govt-takes-down-thousands-of-deepfake-accounts-contents-ahead-of-regional-elections>, last accessed 5 January 2026.
- ³⁶ Manila Standard, *CICC warns about rising threat of deepfakes, cyberattacks ahead of elections*, March 2025, <https://manilastandard.net/business/314568873/cicc-warns-about-rising-threat-of-deepfakes-cyberattacks-ahead-of-elections.html>, last accessed 5 January 2026.

-
- ³⁷ The Straits Times, *How 10 blocked websites masquerade as authentic Singapore news sites*, October 2024, <https://www.straitstimes.com/singapore/how-10-blocked-websites-masquerade-as-authentic-singapore-news-sites>, last accessed 5 January 2026.
- ³⁸ HP Wolf Security, *HP Wolf Security Threat Insights Report: September 2024*, <https://threatresearch.ext.hp.com/hp-wolf-security-threat-insights-report-september-2024/>, last accessed 5 January 2026.
- ³⁹ Source: INTERPOL questionnaires and consultations with law enforcement agencies from Southeast Asia.
- ⁴⁰ The information provided in this sub-section regarding tools has been acquired through interviews and consultations with INTERPOL member countries.
- ⁴¹ Manila Bulletin, *Gov't launches anti-deepfake task force, AI tool*, March 2025, <https://mb.com.ph/2025/3/19/govt-launches-anti-deepfake-taskforce>, last accessed 5 January 2026.
- ⁴² HTX, *Fighting the scourge of deepfakes with AlchemiX*, April 2024, <https://www.htx.gov.sg/whats-happening/all-news---events/all-news/2024/featured-news-fighting-the-scourge-of-deepfakes-with-alchemix>, last accessed 5 January 2026.
- ⁴³ The Philippine Star, *Report scams to hotline 1326 – CICC*, November 2024, <https://www.philstar.com/nation/2024/11/11/2399174/report-scams-hotline-1326-cicc>, last accessed 5 January 2026.
- ⁴⁴ Brunei Darussalam Central Ban (BDCB), *Beware and Stay Alert of Fake News Generated By Artificial Intelligence (AI)*, June 2024, <https://www.bdc.gov.bn/publications/details?id=01j0ac4vr3qecm7g930yq922yv>, last accessed 5 January 2026.
- ⁴⁵ BCA Always by your side, *Beware of Deepfake AI Scams*, May 2025, <https://www.bca.co.id/en/informasi/awas-modus/2025/05/15/03/03/awas-modus-penipuan-deep-fake-ai>, last accessed 5 January 2026.
- ⁴⁶ Antara Indonesian New Agency, *Indonesia warns public of AI-driven scams, including deepfakes*, April 2025, <https://en.antaranews.com/news/351601/indonesia-warns-public-of-ai-driven-scams-including-deepfakes>, last accessed 5 January 2026.
- ⁴⁷ GovInsider, *Indonesian government encourages ethical AI to tackle deepfakes*, June 2024, <https://govinsider.asia/intl-en/article/indonesian-government-encourages-ethical-ai-to-tackle-deepfakes>, last accessed 5 January 2026.
- ⁴⁸ Malaymail, *Police warn of deepfake scams featuring PM Anwar, Trump, Elon Musk and Teresa Kok*, March 2025, [Police warn of deepfake scams featuring PM Anwar, Trump, Elon Musk and Teresa Kok | Malay Mail](https://www.malaymail.com/news/malaysia/2025/03/03/police-warn-of-deepfake-scams-featuring-pm-anwar-trump-elon-musk-and-teresa-kok), last accessed 5 January 2026.
- ⁴⁹ Media Rujukan Massa Portal berita No. 1 di Malaysia, *Lapor polis jika jadi mangsa 'deepfake' - Bukit Aman*, July 2024, <https://www.bharian.com.my/berita/kes/2024/07/1271808/lapor-polis-jika-jadi-mangsa-deepfake-bukit-aman>, last accessed 5 January 2026.
- ⁵⁰ The Nation Thailand, *Don't fall for 'Deepfake' video calls from scammers: police*, April 2022, <https://www.nationthailand.com/in-focus/40015069>, last accessed 5 January 2026.
- ⁵¹ Bangkok Post, *Deepfake AI scams set to surge in 2024*, December 2023, <https://www.bangkokpost.com/thailand/general/2709134/deepfake-ai-scams-set-to-surge-in-2024>, last accessed 5 January 2026.
- ⁵² Republic of The Philippines Cybercrime Investigation and Coordination Center, June 2025, <https://cicc.gov.ph/>, last accessed 5 January 2026.
- ⁵³ Facebook, Cybercrime Investigation and Coordinating Center – CICC, June 2025, <https://www.facebook.com/CICCGovph/videos/1089184706396995>, last accessed 5 January 2026.
- ⁵⁴ Source: INTERPOL virtual and in-person consultations with government agencies, law enforcement agencies and civil society groups from the Philippines.
- ⁵⁵ Money Authority of Singapore, *Joint Advisory on Scams Involving Digital Manipulation*, March 2025, <https://www.mas.gov.sg/news/media-releases/2025/joint-pnr-by-spf-mas-and-csa>, last accessed 5 January 2026.
- ⁵⁶ ScamShield, *I can ACT against scams Campaign*, January 2023, <https://www.scamshield.gov.sg/i-can-act-campaign/>, last accessed 5 January 2026.
- ⁵⁷ Cyber Security Agency of Singapore (CSA), *Advisory on Detecting and Responding to Deepfake Scams*, March 2024, <https://www.csa.gov.sg/alerts-and-advisories/advisories/ad-2024-006>, last accessed 5 January 2026.

-
- ⁵⁸ ScamShield, *What is ScamShield?*, January 2023, <https://www.scamshield.gov.sg/about-scamshield/#:~:text=We%20value%20and%20respect%20your,any%20known%20signs%20of%20scams>, last accessed 5 January 2026.
- ⁵⁹ Source: INTERPOL questionnaires and virtual consultations with the Singapore Police Force.
- ⁶⁰ Source: INTERPOL virtual and in-person consultations with government agencies, law enforcement agencies and civil society groups from the Philippines.
- ⁶¹ Source: INTERPOL questionnaires and virtual consultations with the Singapore Police Force.
- ⁶² Thai Times, *Covering the Thai Renaissance, Indonesian Civil Society Organizations Combat Deepfake Misinformation in Elections*, February 2026, <https://thaitimes.com/indonesian-civil-society-organizations-combat-deepfake-misinformation-in-elections>, last accessed 5 January 2026.
- ⁶³ Republic of the Philippines, Philippine News Agency, *Task Force 'KKK sa Halalan' formed vs AI-driven mis/disinformation*, July 2024, <https://www.pna.gov.ph/articles/1229400>, last accessed 5 January 2026.
- ⁶⁴ The Straits Times, *Finance director nearly loses \$670k to scammers using deepfakes to pose as senior execs*, April 2025, <https://www.straitstimes.com/singapore/finance-director-nearly-loses-670k-to-scammers-using-deepfakes-to-pose-as-company-senior-execs>, last accessed 5 January 2026.
- ⁶⁵ Singapore Police Force, Police News Releases, *435 Persons Arrested And 109 Investigated In Cross-Border Operation Targeting Online Child Sexual Exploitation Activities*, April 2025, https://www.police.gov.sg/media-hub/news/2025/04/20250404_435_persons_arrested_and_109_investigated_in_cross_border_operation, last accessed 5 January 2026.
- ⁶⁶ Source: INTERPOL questionnaires and consultations with law enforcement agencies from Southeast Asia.
- ⁶⁷ INTERPOL, 2024.
- ⁶⁸ INTERPOL, *How we work, Innovation, Projects, Project SynthWave*, <https://www.interpol.int/en/How-we-work/Innovation/Projects/Project-SynthWave>, last accessed 5 January 2026.
- ⁶⁹ INTERPOL, *News and Events, INTERPOL releases new information on globalization of scam centres*, June 2025, <https://www.interpol.int/en/News-and-Events/News/2025/INTERPOL-releases-new-information-on-globalization-of-scam-centres>, last accessed 5 January 2026.
- ⁷⁰ INTERPOL, *How we work, About Notices*, <https://www.interpol.int/en/How-we-work/Notices/About-Notices>, last accessed 5 January 2026.
- ⁷¹ INTERPOL, *How we work, Databases*, <https://www.interpol.int/en/How-we-work/Databases>, last accessed 5 January 2026.



ABOUT INTERPOL

INTERPOL's role is to enable police in our 196 member countries to work together to fight transnational crime and make the world a safer place. We maintain global databases containing police information on criminals and crime, and we provide operational and forensic support, analysis services and training. These policing capabilities are delivered worldwide and support four global programmes: financial crime and corruption; counter-terrorism; cybercrime; and organized and emerging crime.

OUR VISION: "TOGETHER AGAINST CRIME"

In a world where crime knows no borders, it is clear that collective action is essential to combating crime effectively. INTERPOL serves as a unifying force that brings together police and stakeholders from around the globe with a shared aim: to tackle crime and create a safer world.