HOME TEAM JOURNAL

Issue no. 14
Aug 2024

by Practitioners, for Practitioners

Youths and Crime
- Porn and Sex Offences
- Scammers and the Scammed
- Vaping and Drug Abuse

Safety More than Deterence: A Commentary on Capital Punishment

The Psychology of Deceit: Case Study of a "Pig-Butchering" Scam Victim

Why People Donate to Terrorist Groups

Stealing National Secrets: Spies & Activists

Vaccinating the Home Team

THE LEADERSHIP INTERVIEW

"Every individual is an asset to us. And headcount is so few and rare these days that we must optimise the potential of every individual. ... But people management can never be a one size fits all approach. People have differing expectations, requirements, aspirations, priorities at different stages of their career."

ERIC YAP
Commissioner of
Singapore Civil Defence Force

Protecting Youths at Risk

HOME TEAM JOURNAL

The *Home Team Journal* is a publication by the Home Team Academy in collaboration with the Ministry of Home Affairs of Singapore and its departments, which are collectively known as the Home Team. It is a journal by practitioners and researchers for practitioners and specialists in safety and security.

All correspondence should be addressed to

HOME TEAM JOURNAL EDITORIAL BOARD
Home Team Academy
501 Old Choa Chu Kang Road Singapore 698928

Those wishing to submit manuscripts should send abstracts of proposed articles to the Editor at **MHA_HT_Journal@mha.gov.sg.**

THE HOME TEAM ACADEMY WOULD LIKE TO THANK THE FOLLOWING FOR THEIR SUPPORT:

Jansen Ang
Singapore Police Force

Leon Chan
Central Narcotics Bureau

Chen Yeang Tat
Home Team Science & Technology Agency

Chua Yeng Eng
Training & Competency Development Division, Ministry of Home Affairs

Ee Kiam Keong
Gambling Regulatory Authority

Rockey Francisco Junior
Singapore Prison Service

Evelyn Ho
Home Team Science & Technology Agency

Majeed Khader
Chief Psychologist, Ministry of Home Affairs

Lian Ghim Hua
Singapore Police Force

Ling Young Ern
Singapore Civil Defence Force

Ng Huey Ling
Yellow Ribbon Singapore

Angeline Ong
Internal Security Department

Ong Choon Beng
Immigration & Checkpoints Authority

Daniel Seet
Singapore Civil Defence Force

CONTENTS

Issue no.14 - August 2024

FOREWORD

THE LEADERSHIP INTERVIEW

YOUTHS AT RISK

DRUG ABUSE

CONTENTS

Issue no.14 - August 2024

TERRORISM

CRIME

INTELLIGENCE LEAKS

EMERGING TECHNOLOGIES

HOMEFRONT INSIGHTS

RECENT PUBLICATIONS

FOREWORD

The Singapore Civil Defence Force (SCDF) turned 35 this year. As a former firefighter who had the privilege of serving as SCDF Deputy Commissioner for Operations & Resilience before I moved to the Home Team Academy in 2021, I celebrate its tenacity in constantly innovating to protect lives and properties. I also mourn its losses. In the last two years, two SCDF officers have fallen while performing firefighting operations, underscoring the risks our officers face every time they are on the job. As SCDF Commissioner Eric Yap says in **The Leadership Interview**, being firefighters "positions us as one of the highest risk takers literally and metaphorically". Every SCDF operation is high risk, he tells *Home Team Journal* Editor Susan Sim, and while "systems have been put in place to make sure that the risks are within acceptable limits and contained", the organisation does not have the luxury of calling a safety time-out when a tragedy strikes as "the public will still encounter emergencies and need our assistance."

This is something every Home Team officer knows well; that even as we grieve for injured or fallen comrades, the work of keeping Singapore safe and secure must go on.

On a personal and professional note, I am pleased that our Home Team leaders have been sitting down for extended conversations with the *Journal*, prepared to discuss their organisational challenges and their personal leadership philosophies. Many department heads rarely give interviews, so it has been a privilege to feature them in the *Journal*. The Leadership Interview series began with Issue 8 in 2019, and as the issues are available on https://www.mha.gov.sg/publications, I urge you, reader, to look for the interviews you missed.

The *Journal*, as always, is a publication dedicated to exploring pressing topics on homefront safety and security, not just from the perspectives of its leaders but also those of its specialist practitioners, psychologists, researchers and strategic partners. This edition is no different; it explores various contemporary topics spanning youth crimes, scams, human trafficking, intelligence leaks, and the evolving landscape of cybercrime and terrorism.

Our cover theme, **Protecting Youths at Risk**, reflects the urgent need to address the various crime-related risks and challenges that young people face today. As Nelson Mandela once said, "The youth of today are the leaders of tomorrow." Although the exact provenance of this quote eludes us, its truth resonates deeply. Understanding what makes our youths vulnerable to crime, illicit drugs and anti-social behaviour and making timely interventions are critically important.

Kicking off the discussion is a comprehensive study on the impact of pornography consumption on youth sexual offending. Authored by Koh Jing Han, Karthigan Subramaniam, Bleston Low and Kwek Boon Siang of the Home Team Psychology Division (HTPD), the article examines the alarming rise in youth sexual crimes linked to exposure to pornography. The authors also discuss preventive measures that parents, educators and policymakers can employ to mitigate these risks.

Another study by Lee Yu Jing, Carolyn Misir and Ken Chen from the Police Psychological Services Department (PPSD) delves into the susceptibility of young adults to scams. Their research investigates the characteristics that make youths vulnerable to victimisation and offending in scam-related crimes. By identifying key factors such as unethical behaviour, impulsivity and online disinhibition, the study aims to develop

a profile of youth scam victims and offenders, offering insights crucial for effective crime prevention and victim support strategies.

However, youths are not merely passive victims of scams. Some of them participate in scam-related activities, too. Clarissa Foo, Kwek Boon Siang, Stephanie Chan, Chen Yongjie, and Wong Jia Wen of HTPD surveyed around 400 Singaporean youths to understand the scale and nature of their experiences with scams and related activities. They discovered that about half of the youths surveyed received recruitment offers from scammers, and a quarter of them took them up, tempted by the idea of easy money without thinking of the consequences.

The growing prevalence of youth vaping, an illegal activity in Singapore, is analysed by Leung Chi Ching and Sherrer See of HTPD, who use a biopsychosocial approach to understand the physical, psychological and social implications of vaping among youths. The authors explore the motivations behind youth vaping, its associated risks, and the potential for this behaviour to lead to other illegal activities. By examining local and global preventive strategies, their article provides a comprehensive overview of effective interventions to curb this trend.

While the drug situation in Singapore remains generally under control, there are worrying trends. The number of drug abusers arrested in 2023 increased by 10% from 2022. Among the new abusers arrested, more than half were below 30 years old. The 2022 Health and Lifestyle Survey (HLS) undertaken by Mythily Subramaniam and her colleagues from the Institute of Mental Health, Nanyang Technological University, Khoo Teck Puat Hospital, and Ministry of Health corroborated this observation. The HLS found that the mean age of onset of drug abuse was 15.9 years.[1]

Home Affairs and Law Minister K Shanmugam, who chairs the Inter-Ministry Committee (IMC) on Drug Prevention for Youths, told Parliament in February this year that to deal with the youth drug situation, the IMC was set up in 2023 to tackle the issue of youth drug abuse with a whole-of-government approach. "There is a slightly more permissive attitude amongst our younger people towards drugs," the Minister noted. "They are sometimes influenced by what they read and see online, the lifestyles promoted by permissive cultures and societies, and the falsehoods that are peddled."

This is concerning given the evidence in several other countries that suggest drug abusers have a higher tendency to engage in criminal behaviour and crime, and that drug consumption and trafficking fuel other crimes.[2]

At the same time, there is constant pressure on Singapore, by several international and local groups, to relent on our zero tolerance policies against drugs. Although recent surveys show that most Singaporeans believe that capital punishment is effective in deterring drug trafficking, the Home Team will always have to raise awareness of the highly negative consequences of illicit drug use. As Euston Quah and Tan Jun Rui from the Economic Growth Centre of Nanyang Technological University point out in a commentary for the Journal, it is important to focus not just on the deterrence effect of capital punishment, but also its safety assurance effect. The Home Team's ability to contribute to the public's sense of safety will in turn contribute to broader societal benefits, which they argue include "increased productivity, enhanced well-being, and strengthened public trust in the government's role in safeguarding society.

Every edition of the *Journal* is designed, one could say, to enhance the safety assurance effect. We hope that this issue's focus on the complex interplay of factors contributing to youth crime will help raise awareness and better inform discussions about the collaborative efforts required to protect youths at risk.

The various aspects of terrorism, a staple feature of the Journal, are addressed by three counter-terrorism practitioners. Noor Huda Ismail of the S Rajaratnam School of International Studies (RSIS)

[1] Drugs Related Findings from IMH Survey, 3 May 2023, Central Narcotics Bureau News Release, https://www.cnb.gov.sg/NewsAndEvents/News/Index/drugs-related-findings-from-imh-study

[2] See Home Team Journal Special Issue: Spotlight on Drugs, January 2020.

examines the narratives used by terrorist groups to raise funds. Pamela Goh of the Singapore University of Social Sciences explains the psycho-social responses of bystanders caught in terrorist attacks, and Gazbiah Sans, a former World Bank consultant, emphasises the importance of gender inclusion in the prevention of violent extremism.

On crime, Stephanie Chan and Kwek Boon Siang of HTPD explain the use of psychological coercion by human trafficking syndicates to manipulate and bind victims to them. They coin the acronym TIED-ME (Trauma Bonding, Isolation, Emotional Distress, Debt Bondage, Manipulation, and Exploitation) to describe the evil means used by human traffickers to enslave their victims. And on the now perennial topic of scams, Low Eu Hian, Tan Wei Liang, Carolyn Misir and Jansen Ang of PPSD offer a detailed case study of a "pig-butchering" scam victim to explain the psychological process underpinning investment scams.

Our focus extends to the cyber realm with an extensive study on cybercrime in the ASEAN region. Helena Yixin Huang of RSIS highlights the need for collaborative efforts to tackle this growing threat. Her colleague, Asha Hemrajani, discusses the threats posed by deep fakes and the ongoing efforts to detect and counteract them.

Not forgetting the more traditional tools of espionage, independent national security researcher Vappala Balachandran, a former spymaster himself, discusses why intelligence leaks occur, ranging from the infiltration of government agencies by friendly and hostile powers, local activist groups, and whistle-blowers to outdated and faulty government procedures for safeguarding national secrets.

To round up the issue, several current and former Home Team Medical Services Division members share their insights into how they overcame policy, strategic, and logistical challenges to roll out the COVID-19 vaccination programme for Home Team officers during the pandemic.

This issue is a testament to the continuous quest for better solutions to the critical issues that confront us today. I extend my gratitude to all contributors for their dedicated service. As we embark on this intellectual journey together, I invite you – our readers – to actively engage with us and the authors. Share your insights, challenge prevailing paradigms, and ignite discussions. Your perspectives enrich our collective understanding.

Let curiosity be our compass and empathy our guiding light.

ANWAR ABDULLAH
Chief Executive
Home Team Academy

THE LEADERSHIP INTERVIEW

with Eric Yap

Commissioner, Singapore Civil Defence Force

"I believe we have to build as best as possible for the challenges of tomorrow. All my actions, all the strategies that we undertake, are about building for tomorrow. … The story of the organisation, the story of the capabilities that we want to build, the organisation's vision – when we embarked on our Transformation 2025, quite certainly, we were the first in the firefighting world to do it."

Fresh from Ulster University with a first class honours degree in mass communications, Eric Yap received two job offers – edit the nightly news on local TV, or fight fires. He decided to be a firefighter because the Singapore Civil Defence Force offered a uniform and a higher salary. And he has not looked back since.

When you join an organisation, he tells *Home Team Journal* Editor **Susan Sim**, "you don't imagine wanting to spend the next thirty years working there. … Then as you do the job, you like the job, you see that things are changing and changing for the better for everyone. It's something that keeps you on the job and doing it because it has meaning."

Now the longest serving head of a Home Team Department, Commissioner Yap has many stories to tell – but not about himself, only of the cutting-edge capabilities SCDF is building to meet the challenges of tomorrow. Describing himself as an introvert, he says that he does not "like to be the central figure in everything. I prefer to be the invisible hand, to make sure that things are going right, and things will remain right. If it is not, let's deal with the matter and get it straightened."

His leadership philosophy is to see himself as one of the runners in a relay race, except he is the one currently holding the baton, which he will have to pass on at some point. "So while I'm running it, I make sure I do it at my fastest speed possible and I do my best at making sure that the rest of the teammates have an advantage."

Like most Home Team agencies, the Life Saving Force, he notes, "thrives most in uncertain times" even though the job of an SCDF officer is very high risk "literally and metaphorically".

All his officers know that they put their lives on the line when they enter a fire and, while some risks can be mitigated by putting in place controls, including the use of protective equipment and personal sensors, no two operations are similar and inflexibility in following SOPs might end up, at times, endangering the safety of the team. The

onus is thus on commanders to read the situation continually and take measures to keep their officers safe. "Things do go wrong occasionally especially in an operation which is dynamic," Yap observes. But there must be accountability, and when something does go wrong, supervising officers will be asked: "have you done your best to have prevented it? … what should we do to correct it and prevent it in the future?"

When tragedy strikes – as it has in recent years – he has to ensure that even as he grieves with the families and colleagues of the fallen, the organisation is still able to "perform as expected" because "people will still have emergencies and continue to need our assistance". As a frontline emergency response organisation, the SCDF does not have the "luxury" of a time-out even as it investigates an incident to ensure it does not recur.

Following is an edited transcript[1] of the *Journal*'s interview with Commissioner Yap:

YOU HAVE TO BE PARTICULARLY CALM AND COMPOSED TO SEE THE END IN THE MIDST OF CHAOS

You joined SCDF in 1993 and served in all the key operational commands. You also had one senior staff posting outside SCDF as Senior Director of the Homefront Security Division. Do you think that your career path prepared you for the job of Commissioner of SCDF?

I had two stints outside of SCDF. One was much earlier on, in my career straight after my fire station posting. So the standard posting would be for one to undergo training and after training, undertake frontline rota officer or rota commander position, as it is now called. I did that and subsequently, I was posted to the Ministry to deal with emergency planning, when it was at the Old Phoenix Park. And I did that for about three years.

You were with CEMPO, which used to run the annual emergency planning exercises? Is CEMPO very good preparation for your career?

Yes, I was with Emergency Planning Division then renamed to CEMPO. I think it gives a comprehensive introduction to the whole-of-government preparedness for NE [National Emergency] matters. And you know, being a new officer straight after a frontline posting, going there, obviously, was a steep learning curve.

I think that in a way, that posting exposed me to the breadth and depth of the entire homefront preparedness. And naturally, at that point in time, that was the flavour of the month, you know, [to work] whole-of-government in so far as our readiness for NE was concerned.

So that was my first posting in MHA. Coming quite specifically to your question whether the command postings, as well as the external postings that I did at MHQ prepared me for the job of Commissioner of SCDF, well, I'd say the job of the Commissioner of SCDF entails a very broad scope well beyond those postings that I did.

What the operational tours and some of the external postings that MHA offered me was the necessary foundation to understand the intricacies and the bread and butter of the job of the Commissioner. But there are many other aspects of the job of the Commissioner that one has to be doing the work to really assimilate the nuts and bolts of it.

I say this because SCDF is not just a frontline emergency response operational agency. We have a regulatory role as well. And that regulatory role interfaces very closely with the building industry professionals of Singapore. And because we play such an important part in the building industry pertaining to fire safety requirements for new constructions, for buildings that are undergoing A&As [additions and alterations], the Commissioner is vested with the authority to approve fire safety plans and it is important for the person to have that depth of understanding in order to execute the role well.

[1] The interview was transcribed by Lim Jing Jing. This transcript has been edited for length and clarity.

The postings that I went through – I had very little exposure to that [regulatory] aspect of work because my deployment had largely been in operations – from fire station commander to division commander to director of operations. I had to learn the other aspects of the job quickly and I had to learn a lot and intensely as I took on this position.

Just before I became the Commissioner, that is returning to SCDF from MHA as senior director of the Homefront Security Division, I was Senior Director (Emergency Services). And that position looked after the entire operations side of the house – EMS, firefighting, rescue, and hazmat operations. Regulating fire safety wasn't then placed under this senior director position. So again, that explains why when I took on this job, that was an area that I had to pay particular attention to and learn fast.

You knew you were being groomed for the top job through your postings. They were making sure that you covered all the bases and probably you would have gone through the regulatory training phase as well, if not for the suddenness of command change?

That's right.

But at the end of the day, you also have to be a firefighter, right? To be Commissioner of SCDF?

I think that's the baseline and that is something that all officers progress through. Many of our officers will rise to become a fire station commander. Some will be selected to become a division commander, then a few to helm the operations department, hazmat department and certain specialist operational units as well, like DART [Disaster Assistance and Rescue Team].

Are you a government scholar?

No, I was never one.

You have a first class degree from Ulster University.

Father and mother scholarship. But I was fortunate enough to be given the Fulbright scholarship when I applied for it, and I accepted that scholarship [for graduate studies in the US].

But you can't really parachute a scholar into the SCDF and make him Commissioner, can you?

I wouldn't want to rule out any possibility but understanding the nature of ops and also the strategies to deal with major fire and rescue operations, crisis, et cetera – it's something that if the person has been through certain milestone postings, that would add a considerable amount of confidence.

And often we say a leader in the SCDF has to be particularly calm and composed, and has to be able to see the end state of affairs in the midst of the chaos that is before that person. The ability to strategise operationally based on available capabilities and resources to deal with an unfolding major incident like the Nicoll Highway collapse in 2004 or the Bukom fire incident in 2011, will be demanding on someone entirely new to the organisation. So I can imagine the challenges the person would be up against.

Key Milestones

1993: Joined the Singapore Civil Defence Force after graduating with a degree in Mass Communications from the University of Ulster, Northern Ireland

1994 – 1995: Served as Rota Officer at Changi Fire Station

1995 – 1997: Seconded to Central Emergency Planning Office, Ministry of Home Affairs

1997: Appointed Officer Commanding, Changi Fire Station

2000: Appointed Head Public Affairs Department, HQ SCDF

2001: Obtained a Master of Arts in Management & Organisation Communications from Emerson College, Boston, on a Fulbright Scholarship

December 2001: Appointed Commander, 1st Civil Defence Division, SCDF

2004: Appointed Director Operations Department, HQ SCDF

2008: Appointed Senior Director, Homefront Security Division, Ministry of Home Affairs

2009: Completed the Stanford Executive Programme at Stanford University

2010: Appointed Senior Director, Emergency Services, HQ SCDF

February 2012: Appointed Commissioner SCDF

Major incidents will continue to occur from time to time. For sure, at a certain juncture of one's career, one would be involved in managing a major incident and that adds a lot of confidence to how you deal with future crises. The end of an operation is, for the SCDF, the start of preparation for the next major incident.

You have to have the operational experience, but also a sense of political acuity because some of your decisions will impact public perceptions? Is that a fair way of putting it?

I think for sure because, you know, every decision that we make will come with a trade-off. And that trade-off is something we have to be very circumspect about to make sure that it's the best considered option at that point in time with the information that we have and we move on that front because it's the one that would have minimal undesirable outcomes.

WE REVIEW OUR SUCCESSION PLANS EVERY YEAR

You are now the longest serving head of department in the Home Team. You've seen many leaders come and go, some under quite unfortunate circumstances. Do you think the public service does a good job of selecting and grooming its leaders?

The system is certainly more systematic today versus, you know, in the past. I say it's more systematic because we look at at least two levels below the current incumbent so far as succession planning is concerned.

And this is something that gives a lot of comfort to many organisations because we know that if any surprise were to take place, we have lined up successors. This succession planning also allows us to prepare individuals through the process of postings and training.

Is it just the Home Team or the entire public service that does succession planning this way?

At MHA we do spend quite a lot of time annually reviewing the succession planning for key appointments in every HTD [Home Team Department]. This systematic process ensures the leadership group in HTDs remain strong and younger officers are adequately prepared for senior leadership positions as they progress in their careers.

So, your leadership group essentially knows who is first among equals, which one will be likely to succeed you when you step down?

Indicatively, I think the different roles and different postings that certain individuals have been through may suggest who might be the potential candidates. However, it remains a decision of the leadership in MHQ.

YOU STAY ON THE JOB BECAUSE IT HAS MEANING

Management guru Howard Gardner says that a leader must have a central story or message that he tells to inspire people so that he can be effective. What is your personal story? What made you take up a career that involves running into a fire when the natural instinct is to run away? Bear in mind you did it after your parents already paid to send you overseas to study.

(Laughs.) My style of leadership is one that I prefer to say less of myself. I do tell stories, not stories about myself, but to tell the story of how I see an end state to initiatives might be. And this is something that happens quite often, whether it's with my leadership team or with a larger group, particularly with regards to new capabilities, infrastructures, and process redesigns.

I find it particularly useful and compelling to get buy-in from the entire organisation – I mean there are many examples, including, more recently, the new capabilities that we are putting in place at the academy.

Our new academy was rebuilt over three phases. Phase 1 completed in 2022, Phase 2 completed last year, and Phase 3 is ongoing at the moment and is expected to complete by October this year. The story to this is the end state capability we want to elevate the SCDF to, one that leverages S&T and human factors in training to optimise responders' performance, and entrenching fire science research to strengthen our practical knowledge, et cetera.

Wait a minute, we are still talking about you. I'm sure you used to do recruitment talks. What do you tell these young people you're trying to recruit to inspire them? Surely you tell them something about yourself, why you joined, why you decided to become a firefighter.

How I became a firefighter and how I came to this job is something that I don't voluntarily tell people. But I've been very candid when asked why I decided to join the SCDF. My reply has always been very frank and candid – because that was then the highest paying job offer.

Really?

Yes, at that point in time, it mattered. Being a young man and entering the workforce with a future ahead, securing a decent income is something that mattered a lot and I thought it was also something that I would be more comfortable in because in a uniformed organisation, things are more systematic, and progression is better structured in so far as career development is concerned.

But how did you even know what jobs were available at the SCDF?

Advertisements! It was a newspaper advertisement and you just put your CV in, and in the early nineties, you mailed it in and subsequent to that, you wait for someone to call you up for an interview.

I also submitted an application to SBC, the Singapore Broadcasting Corporation. I also attended an interview with SCDF.

I was offered the SBC position. SCDF was the second one that came back to me with an offer. And as I mentioned, the pay seemed good. It was a no brainer for me at that time to go for SCDF.

The SBC post was for –

It was a news editor position. Night news editor.

What a contrast! One you're sitting behind the desk, the other one, you're fighting fires!

(Laughs.) Yeah, to me a uniform and pay were what mattered then.

You were familiar with the uniformed culture because of national service?

I was in the army for national service. And I quite liked it. Not difficult for me to adjust and adapt to regimentation. At the point in time when you step into an organisation, you don't imagine wanting to spend the next thirty years working there. That wouldn't be foremost on one's mind. It's just coming into the organisation and seeing what it holds.

Then as you do the job, you like the job, you see that things are changing and changing for the better for everyone. It's something that keeps you on the job and doing it because it has meaning.

Your advertisements for SCDF on Facebook start with "choose your adventure". Are you looking for people with a sense of adventure?

That's to appeal to today's audience because today's recruitment ads centre a lot on avatars, right? In this series, we used the avatar of the male and female character, almost designing it along the lines of a virtual game for today's generation. We thought the adventure theme would appeal and designed it based on the concept of a virtual game.

And, of course, the vocations that we offer, the nature of job and experiences we offer also fit nicely into this theme and this concept of "choosing your adventure". If you choose the adventure as an EMS as your experience, you need certain qualities. If you choose an adventure as a fire rescue officer, you need these particular qualities and you can expect these experiences as well.

What about the print advertisement you saw that made you apply to SCDF?

It was very basic. It was very, very basic. (Laughs.) Civil defence officer – that was who they were looking for. I don't think it even said "fire rescue officer". I mean, at that point in time, civil defence had just integrated as an organisation with the fire service in 1989. And the ad I saw was three, four years after integration.

After integration with the Singapore Fire Service, the new organisation was called SJCDF with "J" representing "Joint". In 1992, it then transited to today's SCDF which I joined a year later in 1993.

Did you have to choose between the different services, whether to be in EMS, Emergency Medical Services, or firefighting?

No, then it was just one route of entry, the firefighting role.

A few batches before mine, the trainees had to choose whether they wanted to become a civil defence officer, or a fire-trained officer. But when I joined, everyone had to go through firefighting training, except female trainees. The women only did part of the course. They would then perform attachment to administrative roles in logistics management, HR management, et cetera, when the men undertook firefighting training. And hence at deployment, first posting, the males would go to the fire station. The females would be posted to staff departments.

That changed maybe four, five years after I joined where males and females would go through the same training, go through the same deployment, take on similar leadership duties.

Do you have problems recruiting women?

No, in fact we have a fairly good number of women officers. Maybe around 15% overall? 15% of our force. Firefighters, senior officers, paramedics. In all and every role, we have female officers.

I think 15% to maybe 18% is fairly healthy and reasonable, considering the very physical nature of our job and the demanding nature of shift duties as well. This figure is high when compared to most of our counterpart organisations.

Do you have women in your leadership group?

We had senior officers who recently retired from the leadership group. Like for instance, my previous director of planning and organisation department, she was a senior assistant commissioner when she retired.

Currently, a few of our fire stations are helmed by female officers.

THE STORIES I WANT TO TELL ARE ABOUT BUILDING FOR TOMORROW

So, what is your personal mantra? Do you have one?

I believe we have to build as best as possible for the challenges of tomorrow. All my actions, all the strategies that we undertake, are about building for tomorrow.

And I have to come back somehow to your question about my personal story. I generally tend to speak less of myself and my personal story but to bring audiences to the story of the organisation, the story of the capabilities that we want to build, and really crediting the efforts of everyone in the organisation, because when we embarked on our Transformation 2025, quite certainly, we were the first in the firefighting world to do it.

One clear example is the Phase 1 of our academy transformation. We built and established this centre that we call ExCEL. It stands for Emergency Responders' Fitness Conditioning and Enhancement Laboratory – ExCEL is the acronym.

We ran a story about ExCEL in the Home Team Journal.

You did. Our partner in that is obviously HTX.

But the truth of the matter, and this is not for glory or anything, is that the concept of ExCEL was finalised even before HTX became an organisation. But HTX, being the S&T agency of the Home Team brought in their expertise that helped us to really accelerate what we were doing by ourselves and that is something which we are extremely grateful for.

And it was also fortuitous that we called it ExCEL with the "x" there, which HTX is very proud of to say that, "yeah, we are involved because there's 'x' there". (Laughs.) But it was just all pure coincidence.

In the firefighting world, we talk about training the skills of individuals. We talk about training the physique of individuals through the progressive nature of training. But there are many aspects of training that we are not

optimising the human body on. And this is something that only science will reveal to us the datapoints for us to focus training on. And this is something that ExCEL is now taking emergency responders' training to another dimension altogether. This is something that is definitely a first in the world that we are doing.

First, we are not talking about just the standard training, about physical training. We are talking about comprehensive training including cognitive abilities now.

At our ExCEL, there is a lab that is devoted to cognitive training. Our people will be put through a virtual scenario, whether it is a rescue scenario or fire scenario, and we observe where the person's eyes are looking at, for instance. To an untrained person, when you see fire, you tend to be looking at the fire itself. But as we train individuals, we want to see the coming together of skillsets. As a professional and as a leader, when you see a fire scenario, you will not just observe the fire. You will actually be looking at the surroundings, the risks, and what they might pose to yourself, your team members and the public that you are rescuing.

You're looking for risks of collapsing structures –

Yeah, so with that eye tracker and the cognitive part, we can see brain activities of individuals that allow us to profile the mental workload associated with the tasks. The eye tracking system enables us to evaluate visual scan patterns for situational awareness. Coupled with the psychomotor vigilance test, we can then identify attention and fatigue changes throughout different task types or training regimes.

Establishing such data allows us to calibrate training type and intensity. In operations, for instance, we will be able to strike at an optimal work-rest cycle for responders which can vary considerably between an Asian physique and others. Aided by technology and the expertise of HTX, we can do it now.

Where does the science come from?

The science comes from the HTX team and partners in the institutes of higher learning.

I mean how do you interpret the results? From the experience of your own officers?

Unfortunately, there are no equivalent datasets from our counterparts or partners for comparison with our range of labs and activities we perform. In fact, we work with a variety of partners including the academia. We've had discussions with the University of Kentucky. Coventry University is another partner whom we

EMERGENCY RESPONDERS' FITNESS CONDITIONING & ENHANCEMENT LAB (ExCEL) – A RESEARCH AND DEVELOPMENT FACILITY IN THE SINGAPORE CIVIL DEFENCE FORCE

Hasen Kuddoos & Melissa Choo
Singapore Civil Defence Force

ABSTRACT

The Emergency Responders' Fitness Conditioning and Enhancement Lab (ExCEL) is an integrated purpose-built facility jointly developed by the Singapore Civil Defence Force and the Home Team Science and Technology Agency to improve the physiological and cognitive performance of emergency responders through training. ExCEL enables end-user research and evidence-based findings to evaluate training effectiveness and efficiency, leading to an improved quantitative profiling of training regimes. In this article, we discuss the comprehensive suite of analysis tools within each walls of ExCEL and how they support operational, research, and conditioning/corrective training functions.

DOUBLING DOWN ON SAFETY AND PERFORMANCE

Emergency responders are often required to attend to cases with agility and strength to mitigate an incident effectively. As the demand for emergency response continues to rise due to Singapore's ageing population, the challenge for the Singapore Civil Defence Force (SCDF) is to boost its ability to respond to rising operational needs with limited resources. There is a need to study how responder performance can be optimised, and to institute a comprehensive and scientific approach to training and operations.

To pursue an objective evaluation of training efficacy, the SCDF doubled-down on its investment in responder safety, health, and performance to build a holistic suite of capabilities housed in the Emergency Responders' Fitness Conditioning and Enhancement Lab (ExCEL). Commissioned and operationalised in 2021, ExCEL resides in the Civil Defence Academy (CDA) as a key feature of its Field Training Area and serves as a focal point for the study of human performance through collaboration with research and industry partners.

ExCEL hosts an array of research thrusts, and looks into the selection and development of responders to improve the suitability of vocation deployment. Through targeted profiling and evaluation, intervention tools are also devised to enhance individual performance and help responders to prevent and recover from injuries. This is carried out through the:

a. Collection and assessment of multi-factorial longitudinal data to monitor various aspects of a responder's performance;
b. Conduct of research and trials for evaluation of training regimes;
c. Implementation of bespoke training regimes – such as heat acclimatisation, aerobic fitness conditioning, functional fitness training – to prepare emergency response trainees for the demands of real operations;
d. Design of psychological tools for the progression of leaders; and
e. Development of digital content to emphasise specific neurocognitive functions for enhanced learning and operational preparedness.

EXCEL Facilities

Covering over 1,200 sqm in built-up area within the CDA, ExCEL houses five installations connected to a central monitoring system. Each installation harnesses its own technology to optimise responder performance and offers numerous research opportunities in the study of human factors.

STRIVE

The Strength Conditioning & Rehabilitation in Virtual Environment (STRIVE) is a state-of-the-art lab that uses a 360-degree interactive and immersive gamified environment for the assessment of human factors and ergonomics, and to provide conditioning for operational and unconventional terrains. A first in the firefighting community, it combines a motion platform with six degrees of freedom, an instrumental dual-belt treadmill, a motion capture system, as well as a visualisation and audio system to provide responders with real-time feedback on their kinetics and kinematics.

Using high-speed cameras and electromyography sensors (which assess the health of muscles and the nerve cells that control them) for performance analyses, STRIVE provides real-time and longitudinal monitoring of a range of human factor indices for a holistic evaluation. As an advanced biomechanics lab, STRIVE offers the following:

a. Situational awareness training for firefighting and rescue operations;
b. Assessment and characterisation of muscle activation patterns in different operational techniques, such as the proper methods to lift heavy equipment and proper running form;
c. Conditioning for uneven terrains, e.g., stimulating rough sea states during motion acclimatisation training for responders in marine units;
d. Evaluation and optimisation of load carriage and exoskeleton systems;
e. Profiling and analysis of responders' gait patterns to predict fatigue rate or injury risks; and
f. Treatment for individuals with Post-Traumatic Stress Disorder (PTSD)

The Strength Conditioning & Rehabilitation in Virtual Environment (STRIVE)

HEAT LAB

The Heat Acclimatisation & Thermoregulation (HEAT) lab features SCDF's new Breathing Apparatus Maze and revamped static stations for

Home Team Journal Issue 12 (February 2023)

have established working committees to explore collaborative projects. EMS training is another dimension which we're considering partnerships with suitable academic institutions. We've had discussions with Monash University.

There are institutes that use bits and pieces of this, but not in its entirety, as we do in the SCDF. Some do it for research while others for different context like in sports. And within the emergency response fraternity, quite certainly, we're the first to push the boundaries in this area of work.

But the data that ExCEL collects is very unique to – I would say not just to SCDF but perhaps on a slightly broader level – Asian emergency responders. This is because of our unique physique compared to say a Caucasian physique. This can translate to important datapoints as emergency responders wear personal protective equipment and carry heavy equipment to perform various tasks. Their agility, gait, endurance, alertness, et cetera, are correlated and the better we understand human factors, the more impactful our training would be to optimise responders' performance.

So the moral of the story is how do we sell this to the organisation, to the everyday firefighters who ask, why do we need such a facility and why do we need to be put through stages of this training?

The reason is that optimal human performance potential of our emergency responders cannot be attained by standard training programme alone and it is also not quantifiable. The future will see skillsets training complemented by programmes leveraging S&T to enable us to develop the physical abilities of individuals optimally.

The datapoints from the five labs of ExCEL and the customised training will enable us to train stronger emergency responders, more resilient emergency responders, and hence, a better prepared one, even though the person may be fresh from school.

And that is one of my stories. I mean, that's one example, but really, we have so many capabilities that the stories just go on and on: how we see the future operating state to be from where we are now.

IT IS NEVER ABOUT THE LEADER

It's a story of how you are changing SCDF. But not the story of why you are doing it.

It's interlinked – it's the 'why' that leads to 'how'. Why we need to do it is important for a reason because obviously, every individual is an asset to us. And headcount is so few and rare these days that we must optimise the potential of every individual.

Take the example of the fire research centre that we built. It is also the first in the world within a fire department. And why we need to do that comes with another story. And another story is about community first responders - why we need to have a strong community first response.

It sounds like your idea of leadership is one where the leader is not someone who is larger than life.

Not necessarily so. I would say that my leadership style is never one that centres around me. It cannot be. Because the organisation must be larger than its individuals.

And the purpose of the larger organisation must take precedence – that's how I've been operating as a leader, if I can be a leader that is not at the front and centre but the functions of the organisation continue to be professionally and seamlessly executed, I would have succeeded very well.

You'll make a terrible politician. I would never vote for you because I wouldn't know you're there.

I will be there when I have to be there but it should never be about me and my leadership style directing this or that. But it is really the collective effort that brought us where we are. And without me, tomorrow the organisation will continue to function absolutely well. And this is something that brings good comfort.

So it is about structures, about systems, about culture.

Yeah, I would agree with you on that. It has to be those aspects that form the foundation of the organisation. Rather than the leader and the leader himself or herself and this is something that

whoever is doing the job can take comfort that structures are in place and things will function well.

However, we do need to ensure good governance, someone to steer the organisation in preparation for future challenges, just like how we are doing it today for tomorrow.

WE HAVE TO TAKE THE RISKS IF THE BUILDING IS BURNING

What about risk taking? I guess there is a sense among some people that most civil servants, even top-level leaders, are quite risk averse. Is that something you agree with? But SCDF obviously cannot be risk averse.

I would say that the nature of our job positions us as one of the highest risk takers literally and metaphorically as well.

Literally, it is self-explanatory because every operation that we embark upon is high risk, but systems are in place to make sure that the risks are within acceptable limits and contained, and where possible, we lower the risks with options that we can implement.

Metaphorically, I suppose the fact is that if we don't take risks and explore out of the box options, the constraints that are surrounding us are quite – quite serious and quite real.

If I could cite an example, for instance, the manpower constraint. It is real in Singapore, real in the public service and naturally that percolates down to individual agencies and SCDF faces it as well. We understand it because the residential labour force isn't going to grow, and will continue to shrink with the ageing population. But the reality is that in our nature of work, where emergency response is concerned, we will need people to be on the ground to deal with all types of emergencies which will continue to occur. You can't have a robot, you can't have AI to replace that paramedic if the person is having a cardiac arrest. You need boots on the ground if you have a burning building, a burning house and this is something that is extremely real.

And we have to confront these issues. And we have to take the necessary risk measures that are fairly unconventional in every sense of the word to tackle these issues.

You also had a couple of tragic incidents where you lost officers—the drowning of Cpl Kok Yuen Chin in a fire station as a result of ragging, the death of Sgt Edward Go while fighting a fire in December 2022. Several SCDF officers have been charged in court in both instances. What were your key concerns in each incident?[2]

The families of the affected, the wellbeing and emotions of immediate families of the affected. The second will certainly be the staff in the organisation and how they see the circumstances and be able to still conduct their everyday duties, perform as expected amidst what had happened. And this is something that I think in some organisations, they may have the luxury of time-out, to call a halt to certain things, suspend certain actions and recalibrate.

But in SCDF operations, even as we grapple with the unfolding situation, we still have to respond to fire incidents and continue – certainly, the public will still encounter emergencies and need our assistance. And how do we then manage the morale, the perception of our people, and the emotions of our people as we grieve. These were topmost of my concerns as the two incidents unfolded.

The officers who were charged – that's a decision the Attorney-General makes. But what sort of message do you send to those in supervisory positions? Is this about taking command responsibility, not failing their men?

Command responsibility is a notion that Minister himself made very clear to the Home Team officers following the 2018 pump well [ragging] incident. And this is something that we try to describe in laymen terms as far as possible to our different levels of leadership to make sure that we understand what

[2] The interview took place before the death of marine rota commander Captain Kenneth Tay while fighting a blaze onboard a tanker on 16 May 2024. The Commissioner's tribute to Cpt Tay was reported by *The Straits Times*, available at https://www.straitstimes.com/singapore/observance-ceremony-held-for-fallen-firefighter-kenneth-tay-30.

is meant by command responsibility, and what it means as we put on our uniform and lead our teams in and outside of operations.

What matters most is that we are fair and just in the way we look at our officers' responses versus what had gone wrong in an operation. But what is also assuring for our people is that within the ambit of an operation, if something did go wrong but they had done their level best based on the information that they had, based on the constraints that they operated within at that point in time, the organisation will not be unfair to the individuals by taking them to task for an operation that did not go as well as it should have been.

In an administrative context, command responsibility carries similar extension. If we take the 2018 episode where what was a celebratory occasion that became a ragging incident leading to the unfortunate death of Cpl Kok – we have always stood firm as a Force on zero tolerance to ragging but it cannot be just an exercise of words on the part of the commanders.

What is important is that commanders must be able to show and demonstrate that they have taken essential measures to make clear the organisation's position on the matter and continually reiterate this from time to time in view of personnel changes.

Having explained to our officers, making sure that every level of command understands command responsibility – it is not about nothing should go wrong when we're on duty. Things can still and will go wrong especially in an operation when surrounding circumstances are so dynamic. Ultimately, it must be: have we done our best to prevent it?

The nature of the job, as you say, is a high-risk vocation. And we talk about bravery of firefighters, paramedics, civil defence. Do you worry that the flip side of bravery if taken to extremes may also create a culture of unnecessary risk-taking?

It's hard for me to describe what is necessary risk and unnecessary risk particularly when we continue to remind our servicemen that no two operations that we undertake are similar. And the reality is to remind everyone that while we have SOPs and we have directives, we can't follow those to the T because the circumstances in operations can be very different and do change by seconds. The rescue strategies we adopt in saving lives can never be risk-free but calibrated. Agility is key and commanders must sense-make and risk assess continually.

So yes, I wouldn't say that risk-taking should be discouraged because, in our profession, the moment we step into the ambulance or the fire engine, the risk is already much higher than a conventional job or responsibility.

Your After-Action Review in 2023 noted that some officers occasionally ignored SCDF's firefighting protocols and SOPs. Why do you think that happened?

We have shared the key findings of the AAR publicly and we must respect that the court process is still ongoing.

One of the AAR findings relate to the use of personal protective equipment, specifically the personal distress device or PDD.

We discovered through our AAR and ground checks that firefighters had generally failed to turn on their PDD when they responded to incidents – perhaps, part forgetfulness, part complacency. And that device, PDD, is motion-triggered. So it's meant to give out a very high decibel sound if no motion is detected for a certain duration of time on an individual to alert the rest of the team that someone needs help. And if you don't turn on that device, no one is going to be aware if a person is in difficulty. And this is something that we discovered, and we had to put it right. So we have implemented stages of checks to ensure complete PPE when teams are dispatched into fire scenes.

Do they not turn on the PDD because they feel they're safe? Complacency often comes from not feeling sufficiently challenged.

No, individuals for sure will recognise the operations that we undertake have got risks and they must protect themselves adequately. However, some may have overlooked the importance as majority of the fire incidents we respond to involve premises that are not complex such as large factory, warehouse, et cetera. Thus, some might have felt that their teammates would be within line of sight. The reality is that regardless of incident types, fires are highly dynamic, and we must regard each uniquely and ensure that we are adequately equipped and protected before tackling it.

But having said that, turning on this device is going to be a thing of the past because the new breathing apparatus that we will be introducing from October this year comes fitted with the device already. So one doesn't need a physical action to turn on the device. The moment a user turns on the breathing apparatus, the device is switched on. We started the procurement process more than two years ago and certainly, before the tragic incident of December 2022.

WE THRIVE MOST IN UNCERTAIN TIMES

The last few years have been very challenging for the Home Team because of COVID-19. So as Singapore's Life Saving Force, what has the experience taught you about leading in such uncertain times? Innovation, management of risks and expectations?

I think we thrive most in uncertain times. I say this not as an individual, but it's really how I see uncertain times—crisis management, disaster management—as a rallying point for the organisation, for uplifting the morale of our people, for really giving the servicemen a focal point to see what this means insofar as all our training is about.

But specifically, during the COVID-19 pandemic, I think we were called to do many things almost overnight from the time when they started to screen passengers on arriving flights in Changi Airport which was shortly after Chinese New Year, in 2020.

They needed a taskforce and SCDF took on one terminal. And we set up our temperature screening and segregation and quarantine services at Terminal 1, Changi Airport. And we did that for, I think, a good two to three weeks.

Subsequent to that, also on short notice, we were informed that our training academy, Civil Defence Academy, would have to accommodate foreign workers because they had to be decanted. So, we had to convert a live training facility to a dormitory and set up a taskforce to manage them. And we did that just over a weekend and on Monday, we started to receive the decanted workers from their dormitories. SCDF undertook many other responsibilities during the pandemic such as training different groups of personnel including PHV [private hire vehicle] drivers and GQF workers in the use of PPEs and basic firefighting skills, manage a GQF [Government Quarantine Facility] at Sembawang, conduct swab testing of people under quarantine, assist in the establishment of various GQFs, transport of persons under quarantine, et cetera – all these at very short notice. These were taskings over and above the everyday emergencies we still had to respond to.

I think the agility of the organisation, to be able to respond to these Whole of Government needs and requests really showed us up in a very proud fashion. I think largely because across the Force, we recognise that it's the crisis agenda that matters most. It's not about whose responsibility it should be, but we are in a crisis, let's deal with the situation because our assistance is needed. We shall take it on and do it well and later on if we need to resolve who should be doing it in the future, or doing it for the long term, we can talk about that separately. But what matters is the situation at hand and we have to deal with the situation well and contain the situation as best as possible.

So I suppose this is linked to the organisation's DNA. SCDF responds to all kinds of emergency, and we are ready every day and always.

In the management of crises, SCDF has not only been training to handle small and large crises at home, but you've also sent teams overseas to help out with earthquakes and disasters, on search and rescue mission, like in Türkiye last year. How is the decision reached as to when the SCDF should send in –

Operation Lionheart.

Is it more determined by foreign policy considerations, or more by what SCDF might be able to contribute and at the same time, learn from the experience? It's training ground, proving ground for your new technologies as well?

I think the driver of it definitely must be the humanitarian dimension. And the practical consideration will be what difference can we bring to a disaster, particularly if it's further away and takes time for us to get there.

And this is something that we have to be very real about it because if it's going to take us more than 36 hours or even 48 hours to get there, the window of opportunity to save lives narrows significantly. And it may not be meaningful for us to go there, as it is not about just being there at the disaster scene. It is about being able to make a difference to those that need rescue assistance.

Do you have many volunteers for such missions?

We have both volunteers and rostered personnel because for us to be able to send out a contingent within four hours of activation, requires us to have a team that is always on standby. And we roster the team every quarterly, and one of the four division commanders will take turns to be the standby commander for that quarter.

Why do it at all?

Humanitarian, as I mentioned. We join the Force, wear the uniform because we believe in its lifesaving mission. You know the humanitarian dimension is very important because we are part of a larger global family. And there is this network – UN International Search and Rescue Advisory Group or INSARAG under the UN OCHA, the Office for the Coordination of Humanitarian Assistance – where Singapore is well regarded for our skills, processes, knowledge and training leadership in disaster response.

The INSARAG secretariat coordinates global response to disasters anywhere in the world. This outreach is done through multiple channels including a dedicated web-based system which certified teams, like SCDF, have access to. And members of this network will then be able to indicate whether they can deploy and if so, details of the rescue contingent.

Is it also very useful for staff morale?

It is. I talked earlier about how managing crises, managing operations becomes a strong rallying point for the organisation because this really underscores all the training we have been providing our people and the scenarios that we train our people on.

And whenever we launch an international mission, the internal audience are very in tune with what we do out there, and the families of our contingent members as well. And we deliberately engage these two groups through different outreach efforts. Regular internal comms is important for our own audience. We also have a team of officers who would volunteer to be the contact point for NOKs [next-of-kins] of the team that is deployed. And this contact point then becomes a focal point providing updates to the family members beyond those that we update on social media. It also serves as an administrative contact point for NOKs as well, to manage any concerns they may have about their loved ones deployed overseas. So, I think that works almost like hand in glove for many of these missions that we have undertaken.

So in any crisis, you don't really have problems trying to maintain staff morale?

No. Actually, crises are events that uplift staff morale significantly. It gives meaning to the job and with very good, clear outcomes. Like for instance, the recent Türkiye deployment [after the February 2023 earthquake in southern and central Türkiye], the two lives that the team saved from the rubble, it's something that, I think everybody was quietly proud of, very quietly proud of.

I was at a conference in Istanbul around the time the mission ended and I showed the audience some photos from the SCDF Facebook. The local Turkish ground commander was wearing an SCDF jacket and hugging the SCDF contingent commander.

We left behind our entire set of personal protective suits for the locals, as a gesture of our goodwill and to wish them strength in recovery from the disaster. The suits protected us and kept our team warm in the colder climes, and we hope they serve the locals likewise.

Prior to the Türkiye deployment, our team also rendered assistance during the floods in New

South Wales. That was just pre-Christmas, 2022. The floods were very bad in New South Wales and the then Commissioner of NSW Fire & Rescue called me to request for assistance in the form of rescuers cum boat technicians. We deployed a contingent of 14 or 15 members for a two weeks' mission.

ROBOTS CAN'T FIGHT FIRES BY THEMSELVES

You've talked about the organisational change the SCDF has been embarking on. What does the future of civil defence look like?

Firefighting and rescue – specifically firefighting and rescue haven't changed much in the last 100 years. Fires are still fought the way it is fought for the reason that the phenomenon of fire hasn't changed. In fact, the threat continues to be challenging, perhaps even more pronounced given the nature of infrastructure design – high rise and subterranean – materials used, et cetera.

Of course, we can control and mitigate many of the risks by having effective fire safety designs in buildings, making sure that if we need to conduct an operation in a high rise building for instance, we can do that expediently and effectively, and the occupants are able to evacuate safely as well.

So, the future of firefighting and rescue, I would say that it wouldn't change dramatically, but it would be complemented by a lot of science and technology in both fire safety systems and emergency response. Passive and active systems will continue to be essential in fire safety designs as they ensure protection for occupants during evacuation and support firefighters in operations. However, we can expect these systems to be enhanced by S&T that can provide early warning to emergency services and occupants when there is a fire. Fire safety standards adopted will also be backed by evidence and research, and this leads me back to one of the earlier points I talked about on the new Fire Research Centre.

In Phase 2 of our academy redevelopment project which we opened last year, we established a fire research centre. It has a 10-megawatt large-cone calorimeter over a volume space where we can erect a 3-storey structure for burn testing. Key datapoints on thermodynamics such as fire development, spread, heat release rate, gas composition, et cetera, will provide us with evidence to reshape our fire code and regulations, and certainly, firefighting strategies.

This is groundbreaking insofar as a fire department is concerned. It will take time to arrive at our intended objectives, but it is something that if we don't start it, we will never arrive there. But if we start it, we possibly can arrive there sooner than never.

We have come really very far from the days when the red rhino was the most innovative thing.

Well, the red rhino continues to evolve – we term that as innovation within an innovation. The sixth generation, which is the latest one, has got three crew and a robot. Yes, it's a three plus one concept in firefighting.

SCDF's 6th Generation Light Fire Attack Vehicle with the Red Rhino Robot (3R) which is able to detect and move towards heat sources autonomously, and spray water and compressed air foam on fires

But you said robots can't fight fires.

Robots can't fight fires, not by themselves as at now. Robots reduce risk and this is something that our people have to be comfortable with, to work alongside robots.

I've got a photo that I can send to you of a completely gutted robot. Had it not been for the robot which penetrated the very large and intense warehouse fire, we would have taken much longer to contain that fire and perhaps, it might even have spread to a neighbouring unit.

That robot suffered quite extensive heat damage from the fire. But that is fine as they are heavy duty and

designed to serve us in such challenging moments which we would have had to commit a lot of manpower and perhaps taken a longer time to deal with.

And that is also one of my stories. When I tell the robot story, it's about why we need to go the robotics way. You look at the robot, it was incinerated. But it was repaired and rebuilt, and today, it's back in operation.

Can you recover the cost from whoever caused the fire? Do we have a system for doing that?

No, we don't cost recover from property owners.

Otherwise, they'd never call you right, when there is a fire.

(Laughs.) Yeah, that's not desirable.

I guess this leads to the question of how SCDF is transforming to meet the future, even though it's a future that's been around for almost the way it's looked for a hundred years, to some extent.

I think digitalisation and use of AI are something that we need to continue to focus on to make sure that the information nodes that come to us will allow us to better sense-make, as we mount the next operation. And this is important because we want to be ahead of the curve, not just as a reactive organisation – it is reactive now because we are called to incidents – but the moment when we are called to incidents, we've got all the key data we need to sense-make and strategise our actions for execution on arrival.

From the dimension of prevention, data analytics can also enable us to be much more targeted in our enforcement functions particularly on the higher risk premises and thereby, reducing the potential for fire incidents to occur.

THE PUBLIC ARE THE FIRST RESPONDERS

You have a story about lifting up the community first response?

Community first responders (CFRs) complement SCDF as they are often in the vicinity of incidents and hence, their proximity can make a difference to those in need before our arrival. Thus, to distinguish their role as first responders, we term SCDF as emergency responders. This differs from the first responder nomenclature which most fire departments call themselves.

Building up the size and competency of CFRs is key to us. For certain, SCDF cannot be everywhere when an incident occurs. During the 8 to 10 mins duration for our response, CFRs can make a real difference in rendering assistance to those in need and helping those around to get out of harm's way.

Bringing the public onboard as CFRs is always work in progress for us. Internally, some 55% to 60% of our people are national service full time personnel. And every quarter I've got a fresh infusion of four, five hundred people into the organisation and the exit of the same number of people - they are new CFRs to our communities.

This is another story with an end state that we aim to achieve which I continue to share with my colleagues – our efforts to build a nation of lifesavers.

The 500 who leave quarterly after they've finished their NS – do they sign up to be your community first responders?

That's an ongoing effort and majority of them are. In this instance, the wider community numbers matter most, and we have a structured approach to that.

For private companies, if their premises are beyond a certain size and occupant load, and in terms of the products they handle like petroleum and flammable materials, they have to have a team of CERT [Company Emergency Response Team] as well. That CERT is also considered as first responders. In fact, they belong to the highest tier as they receive professional training and require annual re-certification. When they are off-duty, they are naturally a trained CFR of the community and we do encourage everyone to register via our myResponder app. If the person chooses not to be an active CFR on our myResponder app, we then encourage him/her to perform as a bystander responder if they were to witness an emergency. Essentially, there's a role for everyone in an emergency and every bit of assistance matters.

For all other companies and community members, we organise regular programmes to engage and train as many as possible in basic lifesaving skills.

Our Transformation 2030 plan, which we will share at our coming Workplan Seminar, will build on the success of our earlier Transformation 2025 plan on the CFR concept.

I mentioned success because we have a network of over 175,000 CFRs on our myResponder app. To date, they have responded to almost 12,000 cardiac arrest and minor fire cases. They have helped save 80 lives and that's 80 loved ones of many families. We are extremely proud of our CFRs.

When it comes to CPR, don't many people decide "I'm trained but I dare not do it in case I'm criticised"?

We continue to assure the public through different means. There will be a group of the public that will be concerned because "I'm not trained, I don't know what to do". But the assurance is that doing something is better than doing nothing at all. For instance, even though you may not have locked your elbows for a perfect CPR, that compression helps blood circulation which has otherwise stopped for a cardiac arrest victim. Every passing minute is 10% less chance of survival for that cardiac arrest patient. CFR or bystander assistance in CPR is key to out-of-hospital cardiac arrest survival.

Being deliberate and instructional, when we receive a 995 call from a bystander, we no longer ask the person, "can you help to do CPR?" Instead, we give instructions: "I need you to help start CPR now." So the response typically will be, "Okay, I can do it", or "I'm not trained, I don't know how to do it." In that case, we tell them, "Put your phone on speaker mode and follow our instructions."

We can also send a GIF to the caller's phone. The GIF will show the action, but on speaker mode, we will guide the person how to do it.

I've seen the response stats. The Home Team Behavioural Sciences Centre was asked to study why people are not responding to myResponder alerts even though they have been trained. And the stats – we ran an article in Home Team Journal – were quite low. Many people said, "Yeah, but if we do it, then all these passers-by look and start commenting."

That's part of our culture. People will take a video and put it on social media.

But again, our assurance is that doing something is definitely better than not doing anything. We also make it a point to present awards in the form of Community First Responder or Community Lifesaver Award to members of the public who have rendered assistance to emergency cases to acknowledge and appreciate their actions, and to encourage others to step forward when it matters most.

NEW KPIS? WE WILL NEVER BE SHORT OF OPERATIONS

What are the wicked problems that SCDF faces?

I talked about manpower constraint. That's a wicked problem to me because you just can't solve it in the conventional sense; if you just don't have the headcount, you can't employ. So you have to look at different options of achieving an outcome with given resources.

We saw it coming in 2014, 2015; that's when we really pushed hard on our Transformation 2025 programme. The concept of CFR is one aspect of our transformation, and another is about sharpening our operational edge with new capabilities through innovation and technological advancement.

Beyond CFR, overall community preparedness for emergencies is equally important. In an emergency situation, one key outcome we seek to achieve is safety for those caught in the vicinity of the incident. Knowing what to do to get out of harm's way and to help others around is important.

Community education in lifesaving skills is a long-term effort and it must start young. This explains our engagement with children as young as K1 level. Simultaneously, we have programmes curated for students in lower and upper primary levels, secondary schools, post-secondary to IHLs. If you will, it's a multi-generational effort which we believe will reap good returns.

And hopefully, with this structure in place, this will be the future of Singapore and the future of our emergency-prepared nation going forward. Ultimately, it is not just about SCDF forces on the ground, but how the community has a role to play in preventing an incident from happening or escalating.

Is there a dilemma too because when you train the public to deal with rubbish chute fires, do CPR, your case numbers will fall. Statistically, as an organisation, you will look like you're doing less. Won't you lose resources then, if the number of fires you're fighting have lowered, and you're in a downward trend?

For fire incidents, just in jest, we probably have to find new KPIs to measure ourselves. But for medical emergencies and rescue operations, those numbers will continue to climb given our ageing population profile.

EMS for sure will be impacted by ageing population. Last year, 65 years old and above comprised almost 50% of our total EMS users. You can imagine what the number would be come 2030 when 1 in 4 of us is going to be 65 and above. This is real and we have been planning for it through a myriad of strategies of managing demand and ensuring there's adequate supply too. Some of these efforts require the involvement of other agencies too.

And fires?

Fires, we have to find new KPIs, you know! While we can eliminate the minor fires such as rubbish chute, rubbish bin fires, that take up 50% of fire call load, the other 50% will continue to occur and pose challenges to us. I shared earlier that the complexity of infrastructure designs will pose challenges to us. And this is real as buildings get taller and basements get deeper and with more use types.

So it is in jest when I say we need to find new KPIs. We will never be short of operations.

Does anything keep you up at night?

Physical exercise is extremely important for my mental balance. So whenever I'm short of that aspect, I can't sleep well. Not so much problems at work. So I have to find time to make sure that I have that balance.

Running is always a pleasure. I run with trainees, I run on my own. If I can, I'll run every day, but time just doesn't permit me.

If there's a major fire at night, do you get a call?

Yes, I do.

Do you go, or do you have to resist the temptation of going?

I have developed such a strong layer of leadership across the division commanders that I don't need to respond as frequently today, as opposed to earlier years, to what we call, "enhanced task force" type of incidents.

There are three levels of incident that we pitch our response to. And these are all pre-determined packages of resources we send out to deal with varying types of incidents.

At the most basic level, this will be a house fire, a shop fire. A basic task force will be sent. Whenever a basic task force is sent, the geographical fire station commander will assume the role of the ground commander and directs the operation.

The next level, when it escalates, say for instance, a factory fire, we dispatch an enhanced task force. And this is when a Division Commander will take charge, the territorial Division Commander. I will usually proceed to these incidents especially if there is a potential for the fire to spread and escalate in scale.

Then the next level is Ops CE level. Ops CE is Ops Civil Emergency. That's the contingency plan that we will activate when we have to deal with large incidents such as Bukom fire in 2011, the Nicoll Highway incident in 2004. That's where the Commissioner himself will take charge.

What are the hard choices you've had to make?

I can't recall any particular examples. But as a commissioner, there will certainly be hard choices we have to make from time to time.

Usually they have to do with people?

Perhaps eighty to ninety per cent. I always tell officers in fireside chats that when we do well in people management, it addresses many of the issues we encounter at work. But it's often easier said than done because people management can never be a one size fits all approach. People have differing expectations, requirements, aspirations, priorities, at different stages of their career.

Besides, it is not possible for policies to meet the needs of everyone. Instead, it should cater to the large majority

based on principled considerations. We then need to do our best in engaging the smaller group separately to help them understand the considerations and the broader objectives the Force seeks to achieve.

IT'S A RELAY RACE AND I HAVE THE BATON NOW

Minister Shanmugam has described your leadership style as one of leading by example, of being focused, determined, knowing what is going on on the ground, not only being able to plan, but good execution as well. Are these the leadership qualities you look for in identifying future leaders for the SCDF?

I cannot expect the next leader to function in the way I am functioning, because every individual has got his or her style of doing things. And there's no one superior way of doing it. There are many roads that lead to the same destination – that is, achieving the mission and vision of the organisation.

And this is something that I've always believed. Obviously, I think what's more important is that the person concerned must have the interest of the larger organisation at heart, focus not just on the here and now, but keeping a keen eye to ready the Force for the future, insofar as what we can see the future to be. For an emergency response organisation like the SCDF, build-up time is necessary when new capabilities are needed as it involves development of a concept of operation, training, equipment acquisition, et cetera. We cannot make up for lost time due to any lack of planning. And this is something that I benefitted from past leaders. And I set myself the expectation to make sure that when the time is right for me to hand over the organisation, the organisation will be in a very good shape for the person to take over and continue to lead it successfully.

I always ask Home Team leaders this question, what is more important to them: to be an effective leader or a moral leader? And almost all will say that you cannot be effective if your personal behaviour undermines respect for your leadership. In the SCDF, you had a previous chief, your predecessor, who was convicted of corruption. How has that experience affected your views on leadership?

I think to err is human. The fact is that we are never perfect individuals. As leaders, we need to continue to reflect on our actions. Actions as in spoken and unspoken. And how we carry ourselves. And be very mindful of what they might mean insofar as the example we want to set as a leader of an organisation.

When the case of my predecessor happened, I think what was important was that we recognised that it was an individual's misjudgement, rather than something systemic. And it certainly doesn't reflect the ethos of the Force and what the rest of the other senior leadership represents, believes in and upholds.

As a leader, I cannot say that being effective is less important, because if we are not an effective leader, our operations will suffer and this impacts our service delivery to the public.

Morally, we have to be on very high ground and this is expected of all leaders. And this is something we need to be constantly mindful of.

Who's the leader you most admire and why?

(Laughs.) I wouldn't say I admire but I found Jack Welch very intriguing. He's a controversial leader but the controversies about his leadership style only emerged after his retirement from GE.

He's the exact opposite of your leadership style!

I don't disagree. There's so much to learn from him. I mean for that 10, 20 years he was at the helm of GE, his style of management was like a celebration of Wall Street. And nobody said a thing about his leadership style then. There were small pockets of people who dissented but everybody saw him as a transformative leader. It was only post-GE, in the later years where people started to analyse his leadership style, that the controversies started to emerge. And it was said that although he built GE from a crumbling organisation to a thriving business at the time of his departure, he actually laid the foundation for its destruction post his retirement. True, untrue, but the reality is that a lot of his corporate philosophy actually continues today in corporate America and the rest of the world.

I mean, for instance, he was best associated with firing unproductive leaders. That was his most well-known corporate strategy, right? Because GE was such a mammoth organisation when he took over with a few hundred thousand employees and he had the unenviable task to restructure it productively by

firing a hundred thousand people in his first year of taking on the CEO position. And today, retrenchment or corporate restructuring continues to be one of the strategies for businesses to realign their focus and trimming costs.

That's not a very relevant message for you.

Perhaps not, especially if it's about relevance to emergency response.

You like the transformative part of him?

There is always something to learn from people in leadership regardless of popularity – these can be teaching moments for me. By reflecting on the styles, decisions made and with the benefit of hindsight, we learn quicker and can avoid walking the path to learn it.

I talked about Welch's approach to retrenchment. He was also an early leader that believed in the concept of outsourcing which is today a common global practice across public and private sectors.

And which the Singapore public service also adopted.

(Laughs.) I mean, obviously his leadership style has got its fair share of shortcomings. For instance, he was short tempered and he led by instilling fear. I would say that these are retrospective analyses of his leadership style. It probably fitted his generation much better than today's generation of course.

But it was not uncommon to see his style of leadership in uniformed organisations in the eighties, nineties, even in the 2000s. To be fair, he turned GE into a highly valuable company in the world then. And as I said earlier, he was then a celebration of Wall Street and his shareholders.

I still don't know what makes you tick. The hints I get from the Jack Welch lessons are what you don't want to be or do. What drives you?

(Pause.) I think the satisfaction from knowing that I have done my level best. As a person, I reflect often on engagements, decisions, and try to be better at it at the next opportunity. From my responses, I guess you could see my introvert nature. And that is why I don't like to be the central figure in everything. I prefer to be the invisible hand, to make sure that things are going right, and things will remain right. If it is not, let's deal with the matter and get it straightened.

I spent much time reading about Jack Welch when I was in school in the UK and later on, when I did my masters at Emerson College – that was almost at the tail end of his GE career. They continued to say good things about him. But post that era, critics become very vocal. But I can understand where the critics are coming from, because you are talking about that generation of 2000, 2010, 2020 and beyond, it's a very different working experience versus the workforce of 1980, 1990 and expectations are very different.

So personally, the style of leadership that I first took on when I was a rota commander or rota officer straight after training has evolved. As a leader, we need to learn continually and adjust and adapt to the operating environment.

I guess people like to read stories. They like to know who is this person, what is this person about. I guess it's a form of assurance that "oh, he's like me" or "this is what I aspire to be".

Maybe it's about connectivity. I'm a pragmatic person, and let me describe it with an analogy – we are in a relay run, even as leaders of the Home Team. At this point in time, I'm holding the baton, I'm running the relay. At some point in time, I have to pass on the baton to somebody else. So while I'm running it, I make sure I do it at my fastest speed possible and I do my best at making sure that the rest of the teammates have an advantage.

And this is what I believe in. This is my philosophy. So it's about building the Force as best as possible, as much as possible, realistically, for the challenges ahead. So that when it's time to hand over, I know things are as best as they can be.

YOUTH PORNOGRAPHY CONSUMPTION AND SEXUAL OFFENDING

Koh Jing Han[1], Karthigan Subramaniam[1], Bleston Low[2] & Kwek Boon Siang[1]
Home Team Psychology Division, Ministry of Home Affairs[1]
& Singapore Prison Service[2]

ABSTRACT

Sexual crimes have been on the rise in Singapore in recent years. There has also been a hike in the number of youth sexual crimes. Studies have identified early and repeated exposure to sexually explicit materials to be one of the contributing factors to youth sexual offending. Several youths arrested for molest in Singapore have also admitted they were acting out fantasies derived from habitual viewing of pornography. This article aims to a) examine the current trends in pornography consumption among youths, b) highlight the potential links between pornography consumption and youth sexual offending, and c) briefly discuss measures that parents and educational institutions may employ to mitigate the risks posed by pornography on youth sexual offending.

SEXUAL OFFENCES IN SINGAPORE

In Singapore, sexual offences are on the rise and have become a cause for concern. In 2022, a five-year high of 2,549 sexual assault cases were reported, including rape, sexual assault by penetration, outrage of modesty (OM) and sexual crime involving children and vulnerable victims (Iau, 2023). In particular, the number of OM cases reported increased from 1,474 cases in 2021 to more than 1,610 cases in 2022 before dipping to 1,528 cases in 2023 (Singapore Police Force, 2024).

Notably, the Report on Youth Delinquency 2021– which defines youth offenders as those between 7 and 19 years old and arrested for crimes other than drug and inhalant abuse – revealed that the number of youths who committed OM and rape offences had increased by 48.6% from 2016 to 2020 (Ministry of Social and Family Development, 2021). In addition, sexual penetration (including sexual penetration of a minor under 16 years of age, which is statutory rape, and exploitative sexual penetration of a minor of or above 16 but below 18 years of age) was the third most common offence committed by youths in Singapore in the same period, the top two offences being theft and cheating.

The rise in youth sexual offending has continued. In 2023, Singapore police arrested more than 470 youths aged 19 and below for sexual crimes, a jump of about 30 per cent in such arrests from 2022 (Lau, 2024).

Two reasons have been offered for this increase: one, youth are being exposed early and repeatedly to sexually explicit materials or adult sexual activity, and two, they are accessing inappropriate or inaccurate information about sexual behaviours and relationships. In combination, sexually explicit material – pornography – could spread misinformation on sex and relationships, causing young men to "adopt unrealistic, harmful perceptions towards women and girls" (Lau, 2024).

The issue is now considered a key priority for the National Committee on Prevention, Rehabilitation and Recidivism (NCPR), which oversees national efforts to prevent offending, re-offending and enhance rehabilitation of offenders. At the NCPR's Conversations on Youth 2023, Senior Parliamentary Secretary for Social and Family Development Eric Chua noted that when he spoke to several youth sex offenders, it was obvious they had had "excessive consumption of pornography". Citing the example of a then 17-year-old who had

been placed on probation for OM offences, Chua said the youth, whom he called 'Adam', had turned his initial curiosity about pornography at 13 years old into "a habitual and monstrous stress coping mechanism that … subsequently led him to act on his thoughts and commit sexual offences." He called for early identification and intervention to steer youths away from offending (Chua, 2023).

This article aims to review existing trends in pornography consumption by youths (defined here as those between 12 and 25 years old), explain the association between pornography use and youth sexual offending, and discuss measures that parents and educational institutions may employ to mitigate the risks posed by pornography on youth sexual offending.

EVOLUTION OF PORNOGRAPHY

Sexually explicit images and writings have existed for millennia. With technology, the creation, distribution, and consumption of such content have evolved significantly. The invention of photography in 1826 led to erotic photos, and they became commercially viable in the 1890s when half-tone printing allowed images to be mass reproduced at lower cost, leading eventually to the creation of pornographic magazines. Motion pictures further revolutionised pornography but such films remained expensive and hard to access. The advent of affordable video cassette recorders in the late 1970s was a game changer, enabling people to purchase or rent pornographic videos and view them in the privacy of their homes. At the same time, cable television networks also started to broadcast soft-core pornography during late-night hours (Weiss, 2020). However, the most significant innovation that drove an exponential growth in pornography consumption is undoubtedly the Internet (Fisher & Barak, 2001), making the pornography industry one of the most lucrative of all time (Keilty, 2018).

In the early 2000s, most pornography sites required consumers to pay subscription fees. However, following the launch of YouTube, the pornography industry adopted the video uploading and streaming model by creating *tube* sites that host user-generated and free content (Fight The New Drug, n.d.-a). These sites offer an immersive environment where viewers can consume unprecedented volumes of pornographic content, facilitated by tags and categories to catalogue available content (Keilty, 2018; Mowlabocus, 2010).

Furthermore, these sites draw on data mined from viewers' browsing patterns to recommend content aligned with their sexual interests, enticing viewers to keep clicking, in hopes of finding their *perfect* clip (Morley, 2022). Today, these tube sites amass the largest viewership within the pornography industry, where viewers are usually presented with shorter clips of hard-core content that can be viewed in quick succession (Forrester, 2016).

Easy access to video recording technology (e.g., smartphones, webcams) and the Internet have made it easier for individuals to create and upload sexual content featuring themselves or others (Fight the New Drug, n.d.-b). This has led to a surge in user-generated videos, commonly known as amateur pornography (Paasonen, 2010). This genre features regular people engaging in private sexual activities filmed using non-professional equipment, and is recognised for its *raw* aesthetic. Thus, amateur pornography is vastly different from high-budget, feature-length productions of commercial pornography that may be perceived as *fake* (Van Doorn, 2010). Amateur pornography appeals to viewers by projecting a fantasy of realness and authenticity, attributable to its low-fi aesthetic and lay performers who have imperfect bodies (Barcan, 2002), whom the viewers, including adolescents, can relate more to (Smith, 2013).

Recent technological advancements (e.g., artificial intelligence [AI], virtual reality [VR]) are transforming the pornography landscape yet again. With the rise of VR pornography (Krueger, 2017), live interactive webcamming (Pezzutto, 2018) and AI-generated pornography (Hunter, 2023), consumers can experience a more immersive and embodied experience.

LAWS INVOLVING OBSCENE MATERIALS IN SINGAPORE

In Singapore, possessing, distributing, producing, or downloading pornographic content is illegal (Singapore Statutes Online, 2023a). Transmitting obscene materials via electronic means is also prohibited (Singapore Statutes Online, 2023b).

In 2022, content creator Titus Low was fined and sentenced to three weeks imprisonment for uploading obscene content onto the online platform *OnlyFans* (Lam, 2022b). His offence only came to light when one of his obscene videos was found on a 12-year-old girl's mobile phone.

This case shows how young people can easily access inappropriate material on their digital devices. This is particularly concerning as a 2019 global survey by Google reported Singaporean children receiving their first Internet-connected device two years earlier than the global average of 10 years old (Tang, 2019). This could explain the prevalence of exposure to pornographic material by Singapore schoolboys. A 2016 survey by Touch Cyber Wellness, which gives online safety talks in Singapore schools, found that nine in every 10 teenage boys in Singapore have watched or read sexually explicit materials within the past year, with some first exposed to pornography even before they started primary school (Tai, 2016).

PORNOGRAPHY CONSUMPTION AMONG YOUTHS

Adolescents have unprecedented access to sexually explicit materials due to the **accessibility**, **affordability and perceived anonymity** offered by the Internet (Cooper et al., 2000) and mobile devices.

Accessibility: With mobile devices, online pornography can now be readily accessed and shared at any time.

Affordability: The overwhelming number of pornography websites has led to intense competition, with some offering reduced access fees or even free content to attract viewers. This is particularly significant for adolescents who may lack financial resources to purchase pornographic content at regular prices.

Perceived Anonymity: The perceived anonymity in online spaces disinhibits individuals, especially adolescents, from engaging in sexual fantasies and experimentation without social deterrence (Quinn & Forsyth, 2005; Young, 2008). The lack of accountability creates challenges for law enforcement as young viewers can easily impersonate older adults to gain access to age-restricted sexual content (Horvath et al., 2013; Shek & Ma, 2016).

Onset and Prevalence of Pornographic Consumption by Youths

Most individuals start watching online pornography during adolescence, with many reporting first exposure prior to the age of 18 (Sabina et al., 2008). The prevalence of youths' pornography use varies worldwide (Peter & Valkenburg, 2016). For example, the prevalence of pornography viewership among adolescents in Asian contexts is generally lower than viewers from Western contexts (Shek & Ma, 2016).

Local research, though limited, shows that most Singaporean boys usually first encounter pornography when they are in upper primary and lower secondary education (Lim et al., 2015; Tai, 2016). A 2016 survey by TOUCH Cyber Wellness found that nine in ten boys aged 13 to 15 have watched or read sexually explicit materials (Tai, 2016).

Although many adolescents seek out sexual content deliberately (Peter & Valkenburg, 2006), unintentional encounters are common as well (Tsaliki, 2011). Western studies indicate that 40-70% of adolescents are initially (and sometimes subsequently) exposed to Internet pornography unintentionally (Peter & Valkenburg, 2016). This can happen for example, when opening unsolicited or spam emails, misspelling searches or accessing pop-up images (Chen et al., 2013; Flood, 2007). In Singapore, a 2014 survey by TOUCH Cyber Wellness suggests that one in three youths between the ages of 13 and 15 has viewed pornography, whether by choice or not (Tai, 2014). Taken together, these findings reflect the significant role the Internet plays in youth pornography consumption, regardless of intentions.

POTENTIAL LINKS BETWEEN PORNOGRAPHY CONSUMPTION AND YOUTH SEXUAL OFFENDING

Adolescence (usually defined as puberty through age 18) is a pivotal period where many undesirable behaviours manifest, and approximately half of sexual offenders report their first offence during this time (Righthand & Welch, 2001). Data from the US indicates that most perpetrators of sexual violence commit their first assault by age 16 (Grotpeter et al., 2008; Ybarra & Mitchell, 2013).

Given that the adolescence period coincides with the ubiquitous habit of pornography consumption,

this section will discuss the existing state of evidence supporting the potential link between pornography use and youth sexual offending in two main areas – pornography use patterns of concern, and formation of unhealthy sexual scripts. The article will then highlight the pathway by which early and frequent pornography consumption, and the possible ensuing formation of unhealthy sexual scripts, can contribute to sexual offending behaviours among youths.

Pornography Use Patterns of Concern

Early Onset of Pornography Use

Young children might struggle to distinguish between fictional pornography and real sexual activities in healthy intimate relationships, leading them to emulate what they see in pornography without fully understanding the consequences (Collins et al., 2017; Martellozzo et al., 2017). With an early exposure to explicit material, children are more likely to engage in sophisticated sexual acts such as sexual intercourse or oral sex (Mesman et al., 2019).

Similar findings have been observed in longitudinal analyses of male adolescents. Those who use sexually explicit media are more likely to engage in oral sex and sexual intercourse compared to their peers who do not consume such media (Brown & L'Engle, 2009; Vandenbosch & Eggermont, 2013). This is similarly reflected in Asian contexts as visits to pornographic sites and engagement in pornographic materials are associated with individuals' sexual debut during their adolescence in Thailand, Taiwan, and Malaysia (Atwood et al., 2012; Cheng et al., 2014; Manaf et al., 2014).

Longitudinal studies have also demonstrated that exposure to pornography during early adolescence predicts the perpetration of sexual harassment (Brown & L'Engle, 2009) and sexually aggressive behaviours in later years (Ybarra et al., 2011). Additionally, research has found that pornography use among sexually active children and adolescents is linked to coerced sexual acts (Alexy et al., 2009), and exposure to pornography prior to the age of 13 may contribute to developing psychopathic and antagonistic attitudes (Hunter et al., 2010).

Given that pornography is found to be one of the most common sources of sexual information for adolescents (Arrington-Sanders et al., 2015; Robb & Mann, 2023), it is possible for young children and youths to internalise various unhealthy sexual scripts, where aggression is endorsed or even encouraged (Shor, 2018). In addition, early exposure to pornography is associated with other undesirable behaviours such as using alcohol and/or drugs during sex (Braun-Courville & Rojas, 2009). These findings have serious implications in Singapore, where it is a punishable offence to have sexual intercourse with persons under 16 years old (Singapore Statutes Online, 2023c), consume alcohol below the age of 18, and consume, traffic, or possess controlled drugs.

Frequency of Pornography Use

The literature consistently shows that frequent use of pornography is associated with sexually permissive attitudes (Braun-Courville & Rojas, 2009; Doornwaard et al., 2015) and more intense objectification of women (Peter & Valkenburg, 2009). Regular users of pornography are more likely to have multiple sexual partners and to engage in a wider range of sexual activities at an earlier age (Donevan & Mattebo, 2017; Rasmussen & Bierman, 2018).

Increased consumption of pornography can shape adolescents' sexual scripts and perceptions of real-life sexual encounters, leading them to perceive pornography as informative and realistic, and to develop a desire to recreate its content (Peter & Valkenburg, 2010; Svedin et al., 2011; Vandenbosch et al., 2018). This partially explains the trend of upskirt or down blouse image-taking of others. These actions are punishable under Section 377BB of the Penal Code (Singapore Statutes Online, 2023d), and Section 30 of the Films Act (Singapore Statutes Online, 2023a). Thus, voyeuristic tendencies are just one example of how increased frequency of pornography use can predispose adolescents to sexual offending.

The pressure to imitate pornography is an aspect of unhealthy relationships (Rothman et al., 2015) that can also lead to the normalisation of coercive sexual acts (Marston & Lewis, 2014). Heavy pornography users tend to rely on pornographic sexual scripts during real-world sexual encounters, possibly due to enhanced salience and accessibility of these scripts with repeated viewings (Bridges et al., 2016; Sun et al., 2016).

The attitudinal and behavioural changes associated with frequent pornography use allude to its addictive potential. It can lead to troublesome consequences such as increased sexual daydreaming (To et al., 2012) and preoccupations with sexual thoughts (Peter & Valkenburg, 2008), which can interfere with daily functioning and potentially contribute to sexual offending. Frequent use can lead to desensitisation to sexual content, requiring increasingly extreme content to achieve similar levels of satisfaction as before (Daneback et al., 2018), which in turn perpetuates the pornography consumption cycle.

Usage of Deviant Content

Early exposure to pornography had been associated with progression to deviant pornography use (Seigfried-Spellar & Rogers, 2013) and subsequent sexual offending (Burton et al., 2010). Deviant, and paraphilic content, which may depict violence or sex involving children and animals, are particularly concerning.

Research suggests that adolescent sex offenders are more likely to have atypical sexual interests, potentially due to repeated exposure to deviant content that alters their sexual arousal patterns (Gan, 2021; Seto & Lalumière, 2010). Watching child pornography, for example, has been linked to a high sex drive (Seto et al., 2010), which is a risk factor related to sexual offending (Seto, 2019). It is important to note that the act of consumption or possession of child sexual abuse materials is punishable under Section 377BK of the Penal Code even when there is no direct sexual contact with a young victim (Singapore Statutes Online, 2023e).

Violent sexual content has strong associations with sexually aggressive behaviours (Hald et al., 2010; Wright et al., 2016), and the intentional consumption of such content predicts an increased likelihood of self-reported sexually aggressive behaviour and perpetration of sexual violence among adolescents such as teen dating violence (Rostad et al., 2019; Ybarra & Thompson, 2018). While the consumption of violent pornography remains relatively low among adolescents (Vandenbosch, 2015; Ybarra et al., 2011), its accessibility and significant associations with aggressive and violent behaviours remain a concern.

Formation of Unhealthy Sexual Scripts (Attitudes and Beliefs)

Several theories that explain the association between pornography use and sexual aggression are rooted in social learning theory (Bandura, 1978, 2001), which postulates that people learn various behaviours by watching and imitating the behaviours of actors, both in real-life and in media. These theories include Simon & Gagnon's (1986) sexual scripts theory and Wright's (2011) sexual script acquisition, activation, and application model of sexual media socialisation (3AM).

Pornography depicts behaviours during sexual encounters that can influence the development of viewers' *sexual scripts* (Simon & Gagnon, 1986). The sexual scripts theories explain sexual activity as learned interactions that follow predictable sequences. These sexual scripts help define what counts as sex, how to recognise sexual situations, and sets up behavioural guidelines for what to do in a sexual interaction (Frith & Kitzinger, 2001).

Through consuming sexual media, viewers can either acquire novel sexual scripts (acquisition) or reinforce existing ones *(activation)*. These scripts then serve as templates for individuals' sexual behaviours (application), as they perceive these behaviours as normative and gratifying (Wright, 2011).

"Physical sexual pleasure over emotional intimacy" scripts

Pornography often depicts sexual encounters that emphasise physical pleasure over emotional intimacy (Katehakis, 2011). This can contribute to the formation of expectations and scripts that may not be compatible with healthy consensual relationships. Such scripts, when coupled with adolescents' increasing use of pornography for sexual arousal and relief through masturbation (Bale, 2011), also limit their self-regulation skills. This in turn may lead to more problematic or compulsive use of pornography (Owens et al., 2012). For example, the reinforcement of pornographic sexual scripts during masturbation can limit adolescents' access to alternative and healthier scripts (Wright, 2011). Furthermore, the dopamine rush experienced during pornography consumption can create unrealistic expectations (Huerta, 2018) about sex with their partners, potentially leading to riskier sexual behaviours that may culminate in sexual offending.

"Sexual Aggression" scripts

Pornography consumption has been associated with increased acceptance of gender-stereotypical sexual beliefs (To et al., 2012; Ward et al., 2015). Pornography often presents gendered sexual scripts, such as male-to-female violence (Klaassen & Peter, 2015) and female degradation (Gorman et al., 2010). For example, almost 90% of the scenes in top-selling pornographic films depict acts of physical aggression, with the most frequently observed acts being spanking and gagging (Bridges et al., 2010). Furthermore, women are predominant targets of sexual and physical aggression, and frequently depicted to respond with pleasure or neutrality (Fritz et al., 2020). Disturbingly, one in eight pornography titles advertised to first-time users describe acts of sexual violence, including scenarios of sexual coercion, exploitation, and sexual assault (Vera-Gray et al., 2021).

Viewers of such content have reported increased endorsement of rape myths, and attitudes supporting violence against women (Rodenhizer & Edwards, 2017). Apart from abusive and violent scripts, pornography often feature other problematic sexual narratives such as the fetishization of incest, infidelity, and the lack of explicit consent communication (Fight the New Drug, n.d.-c; Miller & McBain, 2022).

The prominence of sexual violence in top-performing pornography sites also has serious implications, especially for first-time users (particularly young viewers) who may be introduced to themes of sexual violence from the outset of their pornography exposure (Vera-Gray et al., 2021). The exposure to and the normalisation of sexual violence may entrench potentially damaging sexual scripts for young viewers, and distort their understanding of the boundary between sex and sexual violence.

"Women Objectification" scripts

Pornography use can play a role in influencing the attitudes of adolescents toward women through intensified objectification of women as entities for male sexual gratification (Wright, 2014; Peter & Valkenburg, 2009; Wright & Tokunaga, 2016), and contributes to the development of aggressive attitudes towards women (Vasquez et al., 2018).

In fact, objectification is seen as the "common thread" connecting various forms of sexual violence (Gervais & Eagan, 2017). Adolescents who objectify women may have less empathy towards them, viewing them as mere objects for sexual gratification. Consequently, this contributes to a lack of respect for consent and an increased likelihood in the justification of or engagement in coercive sexual acts (Seabrook et al., 2019). Examples of related non-consenting sexual behaviours are pressuring a partner into kissing, touching or intercourse (Stanley et al., 2018), touching or brushing up against a schoolmate in a sexual way (Brown & L'Engle, 2009), engaging in forced sexual acts (e.g., digital or oral penetration; Alexy et al., 2009), and kissing, touching, or doing anything sexual with another person when that person does not want to do so (Ybarra et al., 2011).

Pathway From Pornography Consumption to Youth Sexual Offending

While the exact causal relationship between pornography consumption and adolescent sexual offending remains uncertain due to limited longitudinal studies, our literature review has uncovered sexual offending risk factors that are also used in established youth sexual violence risk assessment instruments such as Estimate of Risk for Adolescent Sexual Offense Recidivism (ERASOR; Worling & Curwen, 2001) and Juvenile Sex Offender Assessment Protocol-II (J-SOAP-II; Prentky & Righthand, 2003). We will now attempt to synthesize the existing state of evidence and illustrate the pathway from pornography consumption and youth sexual offending.

First, early onset of pornography consumption – particularly before the age of 13 – appears to increase the risk of youths engaging in underage sexual activities, sexual victimisation, involvement in other anti-social activities, and sexually aggressive or deviant behaviours in later years.

Second, early onset of pornography consumption may increase the risk of more frequent pornography consumption. This will likely result in youths developing a preoccupation with sexual thoughts, and seeking sexual gratification and stress coping through masturbation to pornography. Coupled with the easy access to pornography, these factors collectively create an addictive cycle and high

frequency of pornography consumption of increasing varied content, potentially including extreme and deviant types.

Third, stemming from the cycle of early and frequent pornography consumption is the possible development of sexual scripts which lead youths to subscribe to unhealthy beliefs that support early initiation of various sexual activities, or use of violence and aggression to obtain sexual gratification. Youths may also form unhealthy expectations of themselves and of the opposite gender, which in turn lead them to prioritise their need for sexual satisfaction over the safety and consent of others. Specifically, pornography use has been associated with unhealthy sexual scripts that emphasise physical pleasure over intimacy and promote sexual aggression and objectification of women. The normalisation of such scripts may be precursors for what may eventually lead to common adolescent sexual offending such as underage sex, voyeurism, and outrage of modesty.

MITIGATING THE RISKS

While a thorough review of effective measures to mitigate the risk of youth sexual offending is not the intent of this report, some strategies will be discussed here. These are interventions that parents and schools can take to supplement law enforcement efforts.

Early Parental Supervision and Engagement

The advent of mobile technologies coupled with an increasing sexual curiosity during adolescence has increased the likelihood of consumption of online pornography at an earlier age. The accessibility and portability of online pornography confers a private and anonymous viewing experience, emboldening children, and adolescents to progressively search for increasingly sexually explicit (and possibly more deviant) content. Moreover, it becomes more difficult for parents to monitor their children's exposure to such materials (Vanden Abeele et al., 2014). As such, parents can consider implementing technological strategies, such as the installation of filtering, blocking, and monitoring software to delay and prevent their children from being exposed to inappropriate materials (Ybarra et al., 2009).

However, employing such strategies may not completely prevent access to online pornography as young people can easily circumvent parental monitoring by simply deactivating the third-party software (Cameron et al., 2005; Hingorani, 2021). Furthermore, parents should be cautioned against being overly restrictive with the Internet access of older adolescents as they might react by become less forthcoming about their online activities. Hence, the emphasis should not only be placed on limiting access, but also providing anticipatory guidance to adolescents on ways to manage exposure to pornography (Hornor, 2020). For example, parents should have candid and age-appropriate discussions with their children about pornographic content (Ang, 2022).

Nonetheless, most parents are often reluctant to discuss sexuality with their children (Malacane & Beckmeyer, 2016). Even if they are open to having these conversations, parents are often at a loss on what to say to their children (Rothman et al., 2017). Thus, educational resources that offer parents guidance on how to initiate and facilitate these conversations will be useful.

Educational Programmes

Considering how attitudinal shifts often precede behavioural changes (Peter & Valkenburg, 2010; Wright, 2012), interventions can adopt a pre-emptive approach by cultivating healthy and respectful attitudes toward sex and the other gender to resist any negative influences from being exposed to pornographic content. Such interventions can further prevent the downstream manifestations of harmful sexual behaviours. Sexuality education programmes should emphasise media literacy by educating students to critically analyse and interpret content presented in pornography.

Discussions should demystify the gap between reality and fantasy in pornographic portrayals of sex, establish realistic expectations for sex and promote understanding of consent (Lim et al., 2016). Schools can consider implementing media literacy programs specifically designed to enhance understanding ill effects of pornography to address its harmful messages (i.e., pornography literacy programmes).

Pilot studies have demonstrated the feasibility and effectiveness of such programmes in attenuating undesirable sexual attitudes (Rothman et al., 2018; Vandenbosch & van Oosten, 2017). In a local context,

it would be optimal to pitch these programmes for students in the upper primary levels or earlier, as this is the age range where Singaporean youths are first exposed to pornography (Tai, 2016).

CONCLUSION

With the advent of the Internet and mobile technologies, youths can easily be exposed to highly sexualised content either intentionally or unintentionally. They are also being exposed at a younger age and have more opportunities to view such content in private, possibly resulting in prolonged periods of undetected consumption – in terms of frequency and content – by their guardians or trusted adults.

Risk factors such as pubertal maturation, impulsive or rule-breaking personality, peer influence, poor family relationships, and exposure to sexualised social media content have been found to be linked to earlier and more frequent use of pornography by youths in the literature. If undetected, persistent and increasing pornography consumption may continue and contribute to youths developing sexual scripts and behavioural problems that eventually result in sexual offending and other forms of crime.

Therefore, to address the sexual offending risks posed by pornography consumption among youths, interventions should go beyond reducing exposure and focus on educating young viewers to engage with sexual media in an informed manner. Efforts should also focus on educating and equipping parents and guardians with knowledge, technological tools, and skills to delay, prevent and reduce their children's exposure to sexualised content in the social media and pornography.

In addition to enhancing sexuality education programmes, educational institutions can also strengthen their syllabus to imbue positive, healthy, and respectful attitudes in children towards themselves, others, intimate relationships, and sex. This approach may serve to prevent the internalisation of harmful messages conveyed in pornography and can avert downstream manifestations of pernicious sexual attitudes and behaviours.

ABOUT THE AUTHORS

Koh Jing Han
was a research intern with the Crime and Forensic Psychology Branch at the Home Team Psychology Division (HTPD). He graduated from the Nanyang Technological University with a Bachelor of Science (Hons) in Biological Sciences and Psychology. He is currently an Investigation Officer with the Singapore Police Force.

Karthigan Subramaniam
is a Psychologist with the Psychological Services Directorate of the Home Team Psychology Division (HTPD) at the Ministry of Home Affairs. His research interests involve vulnerable victims, sexual crimes, and crime prevention. He has also presented his research findings at various conferences and trains law enforcement officers on topics related to investigative interviewing and crime-related topics.

Bleston Low
is a Psychologist in the Sexual Violence Unit of the Singapore Prison Service. He delivers group and individual psychological assessment and intervention for adults convicted of sexual offences. He is also involved in the evaluation of intervention programme for sexual offending, and his research interests include technology-facilitated sexual violence and youth sexual offending.

Kwek Boon Siang
is a Principal Psychologist who has been with the Ministry of Home Affairs for more than 15 years. He currently holds the appointment of Deputy Director of the Crime and Forensic Psychology Branch at the Home Team Behavioural Psychology Division (HTPD). His research interests are in violent and sexual crimes, offender risk assessment and rehabilitation, scams, and frontline officers' stress and resilience.

REFERENCES

Alexy, E. M., Burgess, A. W., & Prentky, R. A. (2009). Pornography use as a risk marker for an aggressive pattern of behavior among sexually reactive children and adolescents. *Journal of the American Psychiatric Nurses Association, 14*(6), 442-453. https://doi.org/10.1177/1078390308327137

Ang, Q. (2022, February 9). Call for parents to go beyond just protection and prepare kids against online grooming, pornography. *The Straits Times*. Retrieved from https://www.straitstimes.com/singapore/parenting-education/call-for-parents-to-go-beyond-just-protection-and-prepare-kids-against-online-grooming-pornography?login=true&close=true

Arrington-Sanders, R., Harper, G. W., Morgan, A., Ogunbajo, A., Trent, M., & Fortenberry, J. D. (2015). The role of sexually explicit material in the sexual development of same-sex-attracted Black adolescent males. *Archives of Sexual Behavior*, 44(3), 597–608. https://doi.org/10.1007/s10508-014-0416-x

Atwood, K. A., Zimmerman, R., Cupp, P. K., Fongkaew, W., Miller, B. A., Byrnes, H. F., … Chookhare, W. (2012). Correlates of precoital behaviors, intentions, and sexual initiation among Thai adolescents. *Journal of Early Adolescence, 32*(3), 364–386. https://doi.org/10.1177/0272431610393248

Atwood, R. M., Beckert, T. E., & Rhodes, M. R. (2017). Adolescent problematic digital behaviors associated with mobile devices. *North American Journal of Psychology, 19*(3), 659–684.

Bale, C. (2011). Raunch or romance? Framing and interpreting the relationship between sexualized culture and young people's sexual health. *Sex Education, 11*(3), 303–313. https://doi.org/10.1080/14681811.2011.590088

Bandura, A. (1978). Social learning theory of aggression. *Journal of Communication, 28*(3), 12-29. https://doi.org/10.1111/j.1460-2466.1978.tb01621.x

Bandura, A. (2001). Social cognitive theory of mass communication. *Media Psychology, 3*(3), 265-299. https://doi.org/10.1207/S1532785XMEP0303_03

Barcan, R. (2002). In the raw: "Home-made" porn and reality genres. *Journal of Mundane Behaviour, 3*(1).

Beyens, I., Vandenbosch, L., & Eggermont, S. (2015). Early adolescent boys' exposure to Internet pornography: Relationships to pubertal timing, sensation seeking, and academic performance. *Journal of Early Adolescence, 35*(8), 1045–1068. https://doi.org/10.1177/0272431614548069

Braun-Courville, D. K., & Rojas, M. (2009). Exposure to sexually explicit web sites and adolescent sexual attitudes and behaviors. *Journal of Adolescent Health, 45*(2), 156-162. https://doi.org/10.1016/j.jadohealth.2008.12.004

Bridges, A. J., Wosnitzer, R., Scharrer, E., Sun, C., & Liberman, R. (2010). Aggression and sexual behavior in best-selling pornography videos: A content analysis update. *Violence Against Women, 16*(10), 1063-1193. https://doi.org/10.1177/1077801210382866

Bridges, A. J., Sun, C. F., Ezzell, M. B., & Johnson, J. (2016). Sexual scripts and the sexual behavior of men and women who use pornography. *Sexualization, Media, & Society, 2*(4). https://doi.org/10.1177/2374623816668275

Brown, J. D., Halpern, C. T., & L'Engle, K. L. (2005). Mass media as a sexual super peer for early maturing girls. *Journal of Adolescent Health, 36*(5), 420–427. https://doi.org/10.1016/j.jadohealth.2004.06.003

Brown, J. D., & L'Engle, K. L. (2009). X-rated: Sexual attitudes and behaviors associated with U.S. early adolescents' exposure to sexually explicit media. *Communication Research, 36*(1), 3-151. https://doi.org/10.1177/0093650208326465

Burton, D. L., Leibowitz, G. S., & Howard, A. (2010). Comparison by crime type of juvenile delinquents on pornography exposure: The absence of relationships between exposure to pornography and sexual offense characteristics 1. *Journal of Forensic Nursing, 6*(3), 121-129. https://doi.org/10.1111/j.1939-3938.2010.01077.x

Cameron, K. A., Salazar, L. F., Bernhardt, J. M., Burgess-Whitman, N., Wingood, G. M., & DiClemente, R. J. (2005). Adolescents' experience with sex on the web: Results from online focus groups. *Journal of Adolescence, 28*(4), 535–540. https://doi.org/10.1016/j.adolescence.2004.10.00

Chen, A. S., Leung, M., Chen, C. H., & Yang, S. C. (2013). Exposure to Internet pornography among Taiwanese adolescents. *Social Behavior and Personality: An International Journal, 41*(1), 157-164. https://doi.org/10.2224/sbp.2013.41.1.157

Cheng, S., (Kuo-Hsun) Ma, J., & Missari, S. (2014). The effects of Internet use on adolescents' first romantic and sexual relationships in Taiwan. *International Sociology, 29*(4), 324–347. https://doi.org/10.1177/0268580914538084

Chua, E. (2023). Opening Rmarks by SPS Eric Chua at Conversations on Youth 2023 on 27 September. Ministry of Social and Family Development. https://www.msf.gov.sg/media-room/article/opening-remarks-by-sps-eric-chua-at-conversations-on-youth-2023-on-27-september

Collins, R. L., Strasburger, V. C., Brown, J. D., Donnerstein, E., Lenhart, A., & Ward, L. M. (2017). Sexual media and childhood well-being and health. *Pediatrics, 140* (S2), S162-S166. https://doi.org/10.1542/peds.2016-1758X

Cooper, A., Delmonico, D. L., & Burg, R. (2000). Cybersex users, abusers, and compulsives: New findings and implications. *Sexual Addiction & Compulsivity: The Journal Of Treatment & Prevention, 7* (1-2), 5-29. https://doi.org/10.1080/10720160008400205

Daneback, K., Ševčíková, A., & Ježek, S. (2018). Exposure to online sexual materials in adolescence and desensitization to sexual content. *Sexologies, 27*(3), e71-e76. https://doi.org/10.1016/j.sexol.2018.04.001

Donevan, M., & Mattebo, M. (2017). The relationship between frequent pornography consumption, behaviours, and sexual preoccupancy among male adolescents in Sweden. *Sexual & Reproductive Healthcare, 12*, 82-87.

Doornwaard, S. M., Bickham, D. S., Rich, M., ter Bogt, T. F. M., & van den Eijnden, R. J. J. M. (2015). Adolescents' use of sexually explicit Internet material and their sexual attitudes and behavior: Parallel development and directional effects. *Developmental Psychology, 51*(10), 1476–1488. https://doi.org/10.1037/dev0000040

Fight the New Drug (n.d.-a). *How does the porn industry make its money today?* Retrieved from https://fightthenewdrug.org/how-does-the-porn-industry-actually-make-money-today/

Fight the New Drug (n.d.-b). *How has pornography changed in the last 10 years?* Retrieved from https://fightthenewdrug.org/how-has-porn-changed-in-the-last-10-years/

Fight the New Drug (n.d.-c). *How porn can distort consumers' understanding of healthy sex*. Retrieved from https://fightthenewdrug.org/how-porn-can-distort-consumers-understanding-of-healthy-sex/

Fisher, W. A., & Barak, A. (2001). Internet pornography: A social psychological perspective on internet sexuality. *The Journal of Sex Research, 38*(4), 312-323. https://doi.org/10.1080/00224490109552102

Flood, M. (2007). Exposure to pornography among youth in Australia. *Journal of Sociology, 43*(1), 45–60. https://doi.org/10.1177/1440783307073934

Forrester, K. (2016, September 19). Making sense of modern pornography. *The New Yorker*. Retrieved from https://www.newyorker.com/magazine/2016/09/26/making-sense-of-modern-pornography

Frith, H., & Kitzinger, C. (2001). Reformulating sexual script theory: Developing a discursive psychology of sexual negotiation. *Theory & Psychology, 11*(2), 209-232. https://doi.org/10.1177/0959354301112004

Fritz, N., Malic, V., Paul, B., & Zhou, Y. (2020). A descriptive analysis of the types, targets, and relative frequency of aggression in mainstream pornography. *Archives of Sexual Behavior, 49*(8), 3041–3053. https://doi.org/10.1007/s10508-020-01773-0

Gan, E. (2021, January 30). Watching porn, getting addicted: Experts tell of cases they've seen and the risks linked to sexual offenders. *TODAY*. Retrieved from https://www.todayonline.com/singapore/watching-porn-getting-addicted-experts-tell-cases-theyve-seen-and-risks-linked-sexual

Gervais, S. J., & Eagan, S. (2017). Sexual objectification: The common thread connecting myriad forms of sexual violence against women. *American Journal of Orthopsychiatry, 87*(3), 226–232. https://doi.org/10.1037/ort0000257

Gorman, S., Monk-Turner, E., & Fish, J. N. (2010). Free adult Internet web sites: How prevalent are degrading acts? *Gender Issues, 27*(3–4), 131–145. https://doi.org/10.1007/s12147-010-9095-7

Grotpeter, J., Menard, S., Gianola, D., & O'Neal, M. (2008). *Sexual violence: Longitudinal, multigenerational evidence from the National Youth Survey*. Retrieved from https://www.ojp.gov/pdffiles1/nij/grants/223284.pdf

Hald, G. M., Malamuth, N. M., & Yuen, C. (2010) Pornography and attitudes supporting violence against women: revisiting the relationship in nonexperimental studies. *Aggressive Behavior, 36*(1), 14-20. https://doi.org/10.1002/ab.20328

Hingorani, S. (2021, September 3). Don't let pornography become your child's default sex educator. *The Straits Times*. Retrieved from https://www.straitstimes.com/opinion/dont-let-pornography-become-your-childs-default-sex-educator?login=true&close=true

Hornor, G. (2020). Child and adolescent pornography exposure. *Journal of Pediatric Health Care, 34*(2), 191-199. https://doi.org/10.1016/j.pedhc.2019.10.001

Horvath, M. A. H., Alys, L., Massey, K., Pina, A., Scally, M., & Adler, J. R. (2013). "Basically…porn is everywhere": A rapid evidence assessment on the effects that access and exposure to pornography has on children and young people. Project Report. Office of the Children's Commissioner for England, London, UK. Retrieved from https://eprints.mdx.ac.uk/10692/1/BasicallypornIseverywhereReport.pdf

Huerta. D. (2018). Effects of porn addiction on a teen brain. *Focus on the Family*. Retrieved from https://www.focusonthefamily.com/parenting/effects-of-porn-addiction-on-a-teen-brain/

Hunter, J. A., Figueredo, A. J., & Malamuth, N. M. (2010). Developmental pathways into social and sexual deviance. *Journal of Family Violence, 25*, 141-148. https://doi.org/10.1007/s10896-009-9277-9

Hunter, T. (2023, February 13). AI porn is easy to make now. For women, that's a nightmare. *The Washington Post*. Retrieved from https://www.washingtonpost.com/technology/2023/02/13/ai-porn-deepfakes-women-consent/

Iau, J. (2023, April 14). Police to launch priority queues for those reporting sexual crimes at neighbourhood centres. *The Straits Times*. Retrieved from https://www.straitstimes.com/singapore/police-to-launch-priority-queues-for-those-reporting-sexual-crimes-at-neighbourhood-centres?login=true&close=true

Katehakis, A. (2011, July 28). Effects of porn on adolescent boys: When porn becomes an adolescent boy's mode of sex education. *Psychology Today*. Retrieved from https://www.psychologytoday.com/intl/blog/sex-lies-trauma/201107/effects-porn-adolescent-boys

Keilty, P. (2018). Desire by design: pornography as technology industry. *Porn Studies, 5*(3), 338-342. https://doi.org/10.1080/23268743.2018.1483208

Klaassen, M. J. E., & Peter, J. (2015). Gender (in)equality in Internet pornography: A content analysis of popular pornographic Internet videos. *The Journal of Sex Research, 52*(7), 721-735. https://doi.org/10.1080/00224499.2014.976781

Krueger, A. (2017, October 28). Virtual reality gets naughty. *The New York Times*. Retrieved from https://www.nytimes.com/2017/10/28/style/virtual-reality-porn.html

Lam, L. (2022a, November 14). Man admits molesting girl on bus after being exposed to such pornography. *Channel News Asia*. Retrieved from https://www.channelnewsasia.com/singapore/man-molest-girl-bus-exposed-pornography-toilet-phone-record-colleague-3069771

Lam, L. (2022b, October 12). OnlyFans creator Titus Low fined over obscene content, gets jail for defying police order. *Channel News Asia*. Retrieved from https://www.channelnewsasia.com/singapore/titus-low-onlyfans-creator-jail-fine-uploading-obscene-content-3003451

Lam T. H., Shi H. J., Ho L. M., Stewart S. M., Fan S. (2002). Timing of pubertal maturation and heterosexual behavior among Hong Kong Chinese adolescents. *Archives of Sexual Behavior, 31*(4), 359-366. https://doi.org/10.1023/A:1016228427210

Lau, Deborah. (2024, April 15). 30% jump in youths arrested for sex crimes in 2023; exposure to explicit material cited as possible factor. *Channel News Asia*. Retrieved from https://www.todayonline.com/singapore/30-jump-sexual-offences-arrests-youths-2023-year-year-2403851

Lim, K. K., Tan, G., & Chu, C. M. (2015). *An investigation into the use of Internet pornography among young Internet users in Singapore*. Asian Conference on Psychology and Behavioral Sciences 2015. Retrieved from https://papers.iafor.org/wp-content/uploads/papers/acp2015/ACP2015_13257.pdf

Lim, M. S., Carrotte, E. R., & Hellard, M. E. (2016). The impact of pornography on gender-based violence, sexual health and well-being: What do we know? *Journal of Epidemiology and Community Health, 70*(1), 3-5. https://doi.org/10.1136/jech-2015-205453

Malacane, M., & Beckmeyer, J. J. (2016). A review of parent-based barriers to parent–adolescent communication about sex and sexuality: Implications for sex and family educators. *American Journal of Sexuality Education, 11*(1), 27-40. https://doi.org/10.1080/15546128.2016.1146187

Manaf, M. R. A., Tahir, M. M., Sidi, H., Midin, M., Nik Jaafar, N. R., Das, S., & Malek, A. M. A. (2014). Pre-marital sex and its predicting factors among Malaysian youths. *Comprehensive Psychiatry, 55*(Suppl. 1), S82–88. https://doi.org/10.1016/j.comppsych.2013.03.008

Marston, L., & Lewis, R. (2014). *Anal heterosex among young people and implications for health promotion: A qualitative study in the UK. BMJ Open, 4*(8), e004996. https://doi.org/10.1136/bmjopen-2014-004996

Martellozzo, E., Monaghan, A., Adler, J. R., Davidson, J., Leyva, R., & Horvath, M. A. H. (2016). 'I wasn't sure it was normal to watch it'. A quantitative and qualitative examination of the impact of online pornography on the values, attitudes, beliefs and behaviours of children and young people. London: Middlesex University. NSPCC. Retrieved from https://learning.nspcc.org.uk/media/1187/mdx-nspcc-occ-pornography-report.pdf

Mesman, G. R., Harper, S. L., Edge, N. A., Brandt, T. W., & Pemberton, J. L. (2019). Problematic sexual behavior in children. *Journal of Pediatric Health Care, 33*(3), 323-331. https://doi.org/10.1016/j.pedhc.2018.11.002

Miller, D. J., & McBain, K. A. (2022). The content of contemporary, mainstream pornography: A literature review of content analytic studies. American *Journal of Sexuality Education, 17*(2), 219-256. https://doi.org/10.1080/15546128.2021.2019648

Ministry of Social and Family Development. (2021). *Report on Youth Delinquency 2021*. Retrieved from https://www.msf.gov.sg/NCPR/Our-Initiatives/Documents/FA_MSF_Report_on_Youth_Delinquency_2021.pdf

Morley, M. (2022, July 29). The UX of porn tube sites are designed for the ultimate money shot. *AIGA Eye on Design*. Retrieved from https://eyeondesign.aiga.org/the-ux-of-porn-tubes-are-designed-for-the-ultimate-money-shot/ /

Mowlabocus, S. (2010). Porn 2.0? Technology, social practice and the new online porn industry. In F. Attwood (Ed.), *Porn.com: Making sense of online pornography (pp. 90-113.)* Peter Lang: New York.

Owens, E., Behun, R., Manning, J., & Reid, R. (2012). The impact of Internet pornography on adolescents: A review of the research. *Sexual Addiction & Compulsivity, 19*(1-2), 99-122. https://doi.org/10.1080/10720162.2012.660431

Paasonen, S. (2010). Labors of love: Netporn, Web 2.0 and the meanings of amateurism. *New Media & Society, 12*(8), 1225-1398. https://doi.org/10.1177/1461444810362853

Peter, J., & Valkenburg, P. M. (2006). Adolescents' exposure to sexually explicit material on the Internet. *Communication Research, 33*(2), 178-204. https://doi.org/10.1177/0093650205285369

Peter, J., & Valkenburg, P. M. (2008). Adolescents' exposure to sexually explicit Internet material and sexual preoccupancy: A three-wave panel study. *Media Psychology, 11*(2), 207–234. https://doi.org/10.1080/15213260801994238

Peter, J., & Valkenburg, P. M. (2009). Adolescents' exposure to sexually explicit Internet material and notions of women as sex objects: Assessing causality and underlying processes. *Journal of Communication, 59*(3), 407-433. https://doi.org/10.1111/j.1460-2466.2009.01422.x

Peter, J., & Valkenburg, P. M. (2010). Processes underlying the effects of adolescents' use of sexually explicit Internet material: The role of perceived realism. *Communication Research, 37*(3), 375–399. https://doi.org/10.1177/0093650210362464

Peter, J., & Valkenburg, P. M. (2016). Adolescents and pornography: A review of 20 years of research. *The Journal of Sex Research, 53*(4-5), 509-531. https://doi.org/10.1080/00224499.2016.1143441

Pezzutto, S. (2018, November 20). Why adult stars rely on camming. *The Conversation*. Retrieved from https://theconversation.com/why-adult-video-stars-rely-on-camming-104758

Prentky, R. A., & Righthand, S. (2003). *Juvenile Sex Offender Assessment Protocol-II. J-SOAP-II Manual*. Bridgewater, MA

Quinn, J. F., & Forsyth, C. J. (2005). Describing sexual behavior in the era of the internet: A typology for empirical research. *Deviant Behavior, 26*(3), 191-207. https://doi.org/10.1080/01639620590888285

Rasmussen, K. R., & Bierman, A. (2018). Risk or release?: Porn use trajectories and the accumulation of sexual partners. *Social Currents, 5*(6), 566-582. https://doi.org/10.1177/2329496518780929

Righthand, S., & Welch, C. (2001). *Juveniles who have sexually offended: A review of professional literature*. Retrieved from https://www.ojp.gov/pdffiles1/ojjdp/184739.pdf

Robb, M. B., & Mann, S. (2023, January 10). Teens and pornography. *Common Sense*. Retrieved from https://www.commonsensemedia.org/sites/default/files/research/report/2022-teens-and-pornography-final-web.pdf

Rodenhizer, K. A. E., & Edwards, K. M. (2017). The impacts of sexual media exposure on adolescent and emerging adults' dating and sexual violence attitudes and behaviors: A critical review of the literature. *Trauma, Violence, & Abuse, 20*(4), 439-452. https://doi.org/10.1177/1524838017717745.

Rostad, W. L., Gittins-Stone, D., Huntington, C., Rizzo, C. J., Pearlman, D., & Orchowski, L. (2019). The association between exposure to violent pornography and teen dating violence in grade 10 high school students. *Archives of Sexual Behavior, 48*, 2137-2147. https://doi.org/10.1007/s10508-019-1435-4

Rothman, E. F., Adhia, A., Christensen, T. T., Paruk, J., Alder, J., & Daley, N. (2018). A pornography literacy class for youth: Results of a feasibility and efficacy pilot study. *American Journal of Sexuality Education, 13*(1), 1-17. https://doi.org/10.1080/15546128.2018.1437100

Rothman, E. F., Kaczmarsky, C., Burke, N., Jansen, E., & Baughman, A. (2015). "Without porn … I wouldn't know half the things I know now": A qualitative study of pornography use among a sample of urban, low-income, Black and Hispanic youth. *Journal of Sex Research, 52*(7), 736–746. https://doi.org/10.1080/00224499.2014.960908

Rothman, E. F., Paruk, J., Espensen, A., Temple, J. R., & Adams, K. (2017). A qualitative study of what US parents say and do when their young children see pornography. *Academic Pediatrics, 17*(8), 844-849. https://doi.org/10.1016/j.acap.2017.04.014

Sabina, C., Wolak, J., & Finkelhor, D. (2008). The nature and dynamics of Internet pornography exposure for youth. *CyberPsychology & Behavior, 11*(6), 691-693. https://doi.org/10.1089/cpb.2007.0179

Seabrook, R. C., Ward, L. M., & Giaccardi, S. (2019). Less than human? Media use, objectification of women, and men's acceptance of sexual aggression. *Psychology of Violence, 9*(5), 536–545. https://doi.org/10.1037/vio0000198

Seigfried-Spellar, K. C., & Rogers, M. K. (2013). Does deviant pornography use follow a Guttman-like progression?. *Computers in Human Behavior, 29*(5), 1997-2003. https://doi.org/10.1016/j.jcrimjus.2011.11.004

Seto, M. C. (2019). The motivation-facilitation model of sexual offending. *Sexual Abuse, 31*(1), 3-24. https://doi.org/10.1177/1079063217720919

Seto, M. C., & Lalumière, M. L. (2010). What is so special about male adolescent sexual offending? A review and test of explanations through meta-analysis. *Psychological Bulletin, 136*(4), 526–575. https://doi.org/10.1037/a0019700

Seto, M. C., Reeves, L., & Jung, S. (2010). Explanations given by child pornography offenders for their crimes. *Journal of Sexual Aggression, 16*(2), 169-180. https://doi.org/10.1080/13552600903572396

Shek, D. T. L., & Ma, C. M. S. (2016). A six-year longitudinal study of consumption of pornographic materials in Chinese adolescents in Hong Kong. *Journal of Pediatric & Adolescent Gynecology, 29*(1, Suppl), S12-S21. https://doi.org/10.1016/j.jpag.2015.10.004

Shor, E. (2018). Age, aggression, and pleasure in popular online pornographic videos. *Violence Against Women, 25*(8), 1018-1036. https://doi.org/10.1177/1077801218804101

Simon, W., & Gagnon, J. H. (1986). Sexual scripts: Permanence and change. *Archives of Sexual Behavior, 15*(2), 97-120. https://doi.org/10.1007/bf01542219

Singapore Police Force. (2024). *Annual Crime Brief 2023*. Retrieved from https://www.police.gov.sg/Media-Room/Statistics

Singapore Statutes Online. (2023a). *Films Act 1981 (SECTION 29 & 30)*. Retrieved from https://sso.agc.gov.sg/Act/FA1981#pr29-

Singapore Statutes Online. (2023b). *Penal Code (CHAPTER 14 SECTION 292)*. Retrieved from https://sso.agc.gov.sg/Act/PC1871?ProvIds=P414_267A-#pr292-

Singapore Statutes Online. (2023c). *Penal Code (CHAPTER 16 SECTION 376A)*. Retrieved from https://sso.agc.gov.sg/Act/PC1871?ProvIds=P416-#pr376-

Singapore Statutes Online. (2023d). *Penal Code (CHAPTER 16 SECTION 377B)*. Retrieved from https://sso.agc.gov.sg/act/pc1871#pr377BB-

Singapore Statutes Online. (2023e). *Penal Code (CHAPTER 16 SECTION 377BK)*. Retrieved from https://sso.agc.gov.sg/act/pc1871?ProvIds=P416-#pr377BK-

Smith, M. (2013). Youth viewing sexually explicit material online: Addressing the elephant on the screen. *Sexuality Research & Social Policy: A Journal of the NSRC, 10*(1), 62–75. https://doi.org/10.1007/s13178-012-0103-4

Stanley, N., Barter, C., Wood, M., Aghtaie, N., Larkins, C., Lanau, A., & Överlien, C. (2018). Pornography, sexual coercion and abuse and sexting in young people's intimate relationships: A European study. *Journal of Interpersonal Violence, 33*(19), 2919–2944. https://doi.org/10.1177/0886260516633204

Sun, C., Bridges, A., Johnson, J. A., & Ezzell, M. B. (2016). Pornography and the male sexual script: An analysis of consumption and sexual relations. *Archives of Sexual Behavior, 45*(4), 983-994. https://doi.org/10.1007/s10508-014-0391-2

Svedin, C. G., Akerman, I., & Priebe, G. (2011). Frequent users of pornography. A population based epidemiological study of Swedish male adolescents. *Journal of Adolescence, 34*(4), 779-788. https://doi.org/10.1016/j.adolescence.2010.04.010

Tai, J. (2014, September 6). Half of teens in Singapore exposed to pornography: Survey. *The Straits Times*. Retrieved from https://www.straitstimes.com/singapore/half-of-teens-in-singapore-exposed-to-pornography-survey?login=true&close=true

Tai, J. (2016, June 29). Nine in 10 teen boys in Singapore exposed to porn: Survey. *The Straits Times*. Retrieved from https://www.straitstimes.com/singapore/nine-in-10-teen-boys-exposed-to-porn-survey?login=true&close=true

Tang, L. (2019, March 18). S'porean children get first Internet device at age 8, among youngest worldwide: Google. *Today*. Retrieved from https://www.todayonline.com/singapore/sporean-children-get-first-internet-device-age-8-among-youngest-worldwide-google

To, S., Ngai, S. S., & Iu Kan, S. (2012). Direct and mediating effects of accessing sexually explicit online materials on Hong Kong adolescents' attitude, knowledge, and behavior relating to sex. *Children and Youth Services Review, 34*(11), 2156–2163. https://doi.org/10.1016/j.childyouth.2012.07.019

Tsaliki, L. (2011). Playing with porn: Greek children's explorations in pornography. *Sex Education: Sexuality, Society and Learning, 11*(3), 293-302. https://doi.org/10.1080/14681811.2011.590087

Vanden Abeele, M., Campbell, S. W., Eggermont, S., & Roe, K. (2014). Sexting, mobile porn use, and peer group dynamics: Boys' and girls' self-perceived popularity, need for popularity, and perceived peer pressure. *Media Psychology, 17*(1), 6–33. https://doi.org/10.1080/15213269.2013.801725

Vandenbosch, L. (2015). Antecedents of adolescents' exposure to different types of sexually explicit Internet material: A longitudinal study. *Computers in Human Behavior, 50*, 439–448. https://doi.org/10.1016/j.chb.2015.04.032

Vandenbosch, L., & Eggermont, S. (2013). Sexually explicit websites and sexual initiation: Reciprocal relationships and the moderating role of pubertal status. *Journal of Research on Adolescence, 23*(4), 621–634. https://doi/org/10.1111/jora.12008

Vandenbosch, L., & van Oosten, J. M. (2017). The relationship between online pornography and the sexual objectification of women: The attenuating role of porn literacy education. *Journal of Communication, 67*(6), 1015-1036. https://doi.org/10.1111/jcom.12341

Vandenbosch, L., van Oosten, J. M., & Peter, J. (2018). Sexually explicit internet material and adolescents' sexual performance orientation: The mediating roles of enjoyment and perceived utility. *Media Psychology, 21*(1), 50-74. https://doi.org/10.1080/15213269.2017.1361842

Van Doorn. N. (2010). Keeping it real: User-generated pornography, gender reification, and visual pleasure. *Convergence, 16*(4), 371-494. https://doi.org/10.1177/1354856510375144

Vasquez, E. A., Ball, L., Loughnan, S., & Pina, A. (2018). The object of my aggression: Sexual objectification increases physical aggression toward women. *Aggressive Behavior, 44*(1), 5-17. https://doi.org/10.1002/ab.21719

Vera-Gray, F., McGlynn, C., Kureshi, I., & Butterby, K. (2021). Sexual violence as a sexual script in mainstream online pornography. *The British Journal of Criminology, 61*(5), 1243–1260. https://doi.org/10.1093/bjc/azab035

Ward, L. M., Vandenbosch, L., & Eggermont, S. (2015). The impact of men's magazines on adolescent boys' objectification and courtship beliefs. *Journal of Adolescence, 39*, 49-58. https://doi.org/10.1016/j.adolescence.2014.12.004

Weiss, R. (2020, July 2). The evolution of pornography. *Psychology Today*. Retrieved from https://www.psychologytoday.com/sg/blog/love-and-sex-in-the-digital-age/202007/the-evolution-pornography

Worling, J. R., & Curwen, T. (2001). Estimate of risk of adolescent sexual offences recidivism (ERASOR; Version 2.0). *Juveniles and children who sexually abuse: Frameworks for assessment, 2*, 372-397.

Wright, P. J. (2011). Mass media effects on youth sexual behavior: Assessing the claim for causality. *Annals of the International Communication Association, 35*(1), 343-385. https://doi.org/10.1080/23808985.2011.11679121

Wright, P. J. (2012). A longitudinal analysis of US adults' pornography exposure. *Journal of Media Psychology, 24*(2), 67-76. https://doi.org/10.1027/1864-1105/a000063

Wright, P. J. (2014). Pornography and the sexual socialization of children: Current knowledge and a theoretical future. *Journal of Children and Media, 8*(3), 305-312. https://doi.org/10.1080/17482798.2014.923606

Wright, P. J., & Tokunaga, R.S. (2016). Men's objectifying media consumption, objectification of women, and attitudes supportive of violence against women. *Archives of Sexual Behavior, 45*, 955–964. https://doi.org/10.1007/s10508-015-0644-8

Wright, P. J., Tokunaga, R. S., & Kraus, A. (2016). A meta-analysis of pornography consumption and actual acts of sexual aggression in general population studies. *Journal of Communication, 66*(1), 183–205. https://doi.org/10.1111/jcom.12201

Ybarra, M. L., Finkelhor, D., Mitchell, K. J., & Wolak, J. (2009). Associations between blocking, monitoring, and filtering software on the home computer and youth-reported unwanted exposure to sexual material online. *Child Abuse & Neglect, 33*(12), 857-869. https://doi.org/10.1016/j.chiabu.2008.09.015

Ybarra, M. L., Mitchell, K. J., Hamburger, M., Diener-West, M., & Leaf, P. J. (2011). X-rated material and perpetration of sexually aggressive behavior among children and adolescents: Is there a link?. *Aggressive Behavior, 37*(1), 1-18. https://doi.org/10.1002/ab.20367

Ybarra, M. L., & Mitchell, K. J. (2013). Prevalence rates of male and female sexual violence perpetrators in a national sample of adolescents. *JAMA Pediatrics, 167* (12), 1125-1134. https://doi.org/10.1001/jamapediatrics.2013.2629

Ybarra, M. L., & Thompson, R. E. (2018). Predicting the emergence of sexual violence in adolescence. *Prevention Science, 19*(4), 403-415. https://doi.org/10.1177/0009922814538700

Young, K.S. (2008). Internet sex addiction: Risk factors, stages of development, and treatment. *American Behavioral Scientist, 52*(1), 21-37. https://doi.org/10.1177/0002764208321339

TOO YOUNG TO BE SCAMMED?
ATTITUDES OF YOUNG ADULTS CONTRIBUTING TO SCAM VICTIMISATION AND OFFENDING

Lee Yu Jing, Carolyn Misir, Ken Chen
Police Psychological Services Department, Singapore Police Force

ABSTRACT

Scams are increasingly prevalent in the digital age, targeting individuals of all ages. While older adults are often considered a vulnerable group, it is important to recognize that even technologically savvy youths can fall victim to scams. In fact, the crime statistics show that young adults in Singapore are more susceptible to scammers than senior citizens. Moreover, a significant proportion of scam offenders are also young adults, with individuals under 30 accounting for about half of the offender population. However, there is a lack of research on the characteristics of youths who are susceptible to both victimisation and offending when it comes to scamming crimes. This study aims to investigate the factors associated with youth scam victimisation and offending to develop a profile of youth scam victims and offenders. Using an exploratory factor analysis, four constructs are found to be important in youth scam attitudes: unethical behaviours, impulsive behaviour, online disinhibition, and personality traits. The findings further show that young adults who engage in scam offences can be predicted by unethical behaviour, online disinhibition, and detachment from victims. These findings are discussed in relation to crime prevention efforts and victimology.

A GLOBAL CONCERN

With greater accessibility and reliance on technology today, there is an increased vulnerability to falling for online scams. In one 12-month period spanning 2022-2023, about a quarter of the global population lost at least US$1.026 trillion (or 1.05% of the global GDP) to scammers, the Global Anti Scam Alliance (GASA) estimates. A non-profit bringing together policy makers, law enforcement, consumer authorities, civil society, the financial sector, cybersecurity, and commercial organisations to share insights and knowledge about scams, GASA found in a 2023 survey of almost 50,000 people from 43 countries that 78% had experienced at least one scam in the last year. While the financial impact varied across countries, the highest average amounts stolen in 2023 affected Singaporeans (US$4,031), the Swiss (US$3,767), and Austrians (US$3,484) (GASA, 2024).

In total, Singaporeans lost S$651.8 million in 2023 to scammers as the number of scam cases spiked by 46.8% to 46,563 in 2023, the Singapore Police Force noted in its Annual Scams and Cybercrime Brief 2023. Even though the authorities have taken measures to warn people against online scams and educate them on how scammers operate, online scam victimisation continues to be on the rise (Singapore Police Force, 2024b).

Consequences of Online Scams

Scams have sometimes been described as a "victimless" crime as some perceive the victim to be responsible in some ways, and that the harm inflicted is trivial, especially when compared to other violent crimes (Duffield & Grabosky, 2001). Contrary to this belief, online scams can have severe, long-term consequences on its victims.

Undoubtedly, the primary and most salient impact of online scams is individuals' financial loss. Financial losses can be extremely debilitating especially for those in a lower income bracket, which is a group that is already vulnerable to online scams (Madden, 2017). After losing their

savings in online scams, victims who are already struggling financially must resort to borrowing money from acquaintances, leading to a further decline in their already low standard of living and strained interpersonal relationships (Wang, 2022). These significant financial losses can even lead to suicidal ideation for some victims, thus highlighting how scams can go beyond financial consequences (Cross, 2018).

Moreover, online scam victimisation can also lead to psychological consequences. Nguyen and colleagues (2021) have demonstrated that scam victims tend to become less trusting of others and assume that people are likely to inflict harm just for their own personal gain. Additionally, victims may lose trust in institutions (e.g., law enforcement agencies, government agencies, technology companies) as they perceive that these entities have not done enough to protect them. However, as it is difficult to assign responsibility to any sole institution for online scam protection, victims often feel a sense of frustration and disappointment as a result (Rhoads, 2023).

Secondly, victims often feel shame and embarrassment from having been scammed, as their beliefs about their own intellect and "common sense" are threatened (Kelley et al., 2012; Nguyen et al., 2021). Many individuals tend to attribute the blame to themselves for being "stupid enough" to fall victim to scams, which subsequently has a detrimental effect on their overall self-worth and self-efficacy (DeLiema et al., 2023). This may result in victims having lower confidence in making decisions, attaining their goals, or even performing tasks (Maddux, 2016). In other words, online scam victimisation can have long-term effects on individuals' functioning and mental well-being, with some victims experiencing post-traumatic stress disorder (PTSD) or anxiety after a victimisation incident (Rhoads, 2023).

While these consequences can arise from all types of online scams, much of the literature highlights the severity of these consequences on online love scam victims. In a study by Whitty and Buchanan (2016), a participant described her experience as akin to being "mentally raped". Some of these participants also considered the emotional impact of losing the relationship to be more distressing than the financial losses incurred. This highlights the significance of the level of intimacy and openness that exists between a scammer and their victim. It is not uncommon for victims to struggle with emotionally detaching from their scammer even after realizing they have been deceived (Chuang, 2021).

YOUTH SUSCEPTIBILITY TO ONLINE SCAM VICTIMISATION

While there are reasons to believe that older individuals are especially susceptible to online scams (e.g., decreased cognitive function, weaker psychological well-being, lower literacy; James, 2014), youths make up the biggest percentage of scam victims. In the US, there was a 116.21% increase in online scam victims under 20 years old in 2020, the highest increase among all age groups (Varga, n.d.). In the Netherlands, people under 35 years old were more likely to be scammed than older people (University of Twente, 2022).

Similarly, 29.2% of scam victims in Singapore in 2023 were under 30 years old, while those above 65 made up 7.1% of the victim population (Singapore Police Force, 2024b). Current research has identified several risk factors that predispose youths to being online scam victims. As the literature primarily use samples that fall within the age range of 18 to 25, the current study will define youths as such.

Environmental Risk Factors

Firstly, **increased exposure to and spending more time on the internet** has been linked to a higher risk of falling victim to scams. Research has demonstrated a clear association between time spent on the internet and negative online interactions. For example, using social networking sites for a longer period increases the risk of being scammed for young people (Kirwan et al., 2018). This can be supported by the routine activity theory, which suggests that crime occurs when there is a "motivated offender, suitable target, and lack of capable guardians" (Holt et al., 2016; Miró, 2014). Spending more time online increases the likelihood that young people, as potential targets, may encounter scammers. Moreover, there may be a lack of sufficient supervision over youths' online activities by their parents, leaving them vulnerable to meeting with negative outcomes online (Liau et al., 2008). Therefore, as young people tend to have higher internet use compared to other age

groups, they may encounter more internet-related problems (Şahin, 2011; Petrosyan, 2024).

Secondly, **engaging in risky or unethical online activities** also increases the likelihood of young people becoming victims of scams. These activities include sharing personal information online, searching for friends online, and illegally downloading music (Choi et al., 2019; Kaakinen et al., 2021). Such activities expose young people to scammers or make them more attractive targets by divulging personal details or visiting sites frequented by scammers (Kaakinen et al., 2021). Additionally, young people may be more willing than other age groups to explore risky online activities due to their limited ability to assess risks and their inclination to interact with others and express themselves online (Bossler & Holt, 2009; Ybarra & Mitchell, 2008). This is further supported by Klapatch et al.'s 2022 study of consumer responses to mass market scam solicitations that found young people to be less likely than older adults to perceive certain types of mass marketing scams as risky. As such, it is not unusual for youths to be more vulnerable to scam victimisation.

Lastly, the concept of **victim-offender overlap** extends its applicability into cybercrime as well, highlighting a correlation between those who fall prey to cybercrimes and those who engage in cybercriminal activities (Burden, 2023). That is, individuals who experience cybercrime victimisation are likely to become perpetrators of cybercrimes, and conversely, those involved in cybercrime offending are predisposed to becoming victims themselves. Moreover, Burden (2023) demonstrates that youths exhibit a higher likelihood of being both victims and offenders, while older adults seem to be more prone to the role of victims without engaging in cybercrime offending activities. The overlap may be attributed to both victims and offenders sharing similar characteristics, such as low self-control (Kerstens and Jansen, 2016). It may also be attributed to pro-criminal cognitions that allow scammers to feel detached from victims. These cognitions can include neutralisation (i.e., putting some blame on the victim or minimising harm to the victim), feelings of entitlement, and revengeful thoughts (Orjiakor et al., 2022).

Dispositional Risk Factors

A dispositional risk factor associated with online scam victimisation among youths is **low self-control** (Kerstens & Jasen, 2016). This could be due to youths not adequately considering the negative effects of their behaviour, tending to engage in risky activities for the thrill, or failing to consistently take precautions that protect them from victimisation (Holt et al., 2016; Schreck, 1999). As such, they are more likely to make decisions that increase the chances of them encountering an online scammer or make themselves more vulnerable to scammers' tactics (Holt et al., 2016).

High online disinhibition has also been linked to victims of scams among youths (Kerstens & Jasen, 2016). Factors leading to online disinhibition, such as increased anonymity and physical invisibility, help people to dissociate their online identities from their offline selves, as well as give them the courage to do things they would not do in real life (Suler, 2004). This can encourage people to take part in risky online activities, which has been linked to falling victim to scams (Choi et al., 2019, Näsi et al., 2015). Online disinhibition can also lead to high online self-disclosure, another risk factor for falling prey to scams (Schouten et al., 2007). For example, youths may also disclose personal information online when forming online friendships to establish trust (Towner et al., 2022), leaving themselves vulnerable to online scammers.

Research has also suggested that **certain personality traits** can increase youths' susceptibility to online scams. Firstly, **introversion** has been linked to greater participation in online activities, such as social media use and gaming, which may increase their exposure to scammers (Choi et al., 2019; Mitchell et al., 2011; Zia & Malik, 2019). Indeed, a study by Kirwan and colleagues (2017) demonstrated that introverted youths were more likely to fall victim to video-type scams than their extroverted peers. However, Modic and Lea (2012) found that extraverted individuals were more impulsive, took more risks, and had greater scam compliance. Extraverted youths are also found to be more prone to sexting, falling victim to online grooming, and online self-disclosure

(Hernández et al., 2021; Peluchette et al., 2015). On the other hand. there are also some studies that suggest extraversion has no significant link to scam victimisation (e.g., Kenninson & Chan-Tin, 2020; Kostić et al., 2016). Thus, the findings of whether the personality trait of introversion/extraversion influences youths' susceptibility to online scams remains mixed and inconclusive.

Another personality trait that has been highlighted is **openness to experience** (Kirwan et al., 2018). Specifically, having a higher score on openness to experience in the Big 5 Personality Traits has been significantly linked to becoming a victim of cybercrime (van de Weijer & Leukfeldt, 2017) and cyberbullying (Peluchette et al., 2015). This may be attributed to heightened curiosity associated with the personality trait, which increases the likelihood of clicking on untrustworthy email attachments (van de Weijer & Leukfeldt, 2017).

In sum, youths have been demonstrated to be more vulnerable to scam victimisation due to external factors such as increased internet exposure and risky online activities. Dispositional factors such as low self-control and high online disinhibition has been associated with scam victimisation among youths, as well as certain personality traits such as introversion, extraversion, openness to experience. Lastly, shared characteristics between victims and offenders influences youths' vulnerability to scam victimisation, giving rise to the victim-offender overlap in cybercrime.

THE PRESENT STUDY

Examining the psychosocial factors contributing to youth involvement in scams can significantly contribute to crime prevention strategies. Existing literature has identified various environmental and dispositional factors contributing to scam victimization. However, there is a need for more research on how youth attitudes specifically contribute to susceptibility as scam victims. As such, this paper aims to further explore the psychosocial variables that influence youths' susceptibility to becoming scam victims based on previous literature. In addition, we examine if these variables are also associated with offending behaviour among youths, as proposed by the victim-offender overlap.

Methodology

We recruited 136 youths between 18 to 25 years old (69.11% females, M*age* = 20.00, SDage = 4.07) to complete a survey on their experiences with online scams. Due to missing data, we only included 131 participants in the final analysis (75.00% females, M*age* = 21.00, SD*age* = 2.06). To measure their personality traits, impulsiveness, and online disinhibition, we asked participants to state how much they agree to modified items adapted from the Ten-Item Personality Inventory (TIPI), 21-item Barratt Impulsiveness Scale (BIS), and the Measure of Online Disinhibition (MOD) scale respectively. Participants then responded to items measuring how often they encountered scams, and their online behaviours (e.g., how long they spend shopping online, texting friends, scrolling through social media, common payment methods, etc.). To measure scam victimisation, we asked if they had been scammed within the past one year, and if so, to elaborate on their experience(s). Next, we measured potential scam offending behaviour by asking participants how much they agreed with the statement "there is no harm done when I prank/trick/scam others on the Internet". We also measured if participants felt detached from victims by asking how much they agree with the sentence "I feel detached from my victim". Finally, they provided their demographic information.

RESULTS

Exploratory Analyses

As this study is exploratory in nature, we conducted an exploratory factor analysis (EFA) across all the items measuring participants' personality traits, impulsiveness, online disinhibition, and online behaviours. We also included the items measuring scam victimisation and offending behaviour. This added up to a total of 84 items that were subjected to promax rotation. To ensure that EFA is an appropriate analysis, we ran a Kaiser-Meyer-Olkin (KMO) test and Barlett's test of sphericity. We obtained a KMO value of 0.53, which falls within the acceptable range (Kaiser, 1974). We also yielded significant results for Barlett's test, χ^2 (df = 3486) = 7866.96, p < .001. This resulted in 9 clusters of interest, with factor loadings ranging from 0.00034 to 0.96.

We removed items that had a factor loading that fell below 0.4 (Pituch & Stevens, 2015) and those that were cross loaded onto more than one factor. However, some items were still included despite having a factor loading that were under 0.4 after exercising some judgement and justifying our choices using internal reliability tests. Also, we excluded items that were outliers within a factor. Therefore, after reviewing each factor and their respective items, we settled on four factors and named it the following: unethical behaviour, impulsive behaviour, online disinhibition, personality traits (refer to Table 1 for a summary of items in each factor).

The factor of unethical behaviour contains 7 items (α = .95) with factor loadings ranging from 0.76 to 0.95. The impulsive behaviour factor contains 9 items (α = .82) with factor loadings ranging from 0.43 to 0.59. The online disinhibition factor contains 8 items (α = .88) with factor loadings ranging from 0.39 to 0.58. There is only one item in this factor that had a factor loading under 0.4 but increased the internal reliability of the factor. Therefore, we decided to retain it. Lastly, the personality traits factor contains 13 items (α = .72) with factor loadings ranging from 0.18 to 0.50. As many items in this factor fall below 0.4, we decided on which items to retain based on those that yielded the highest internal reliability. These factors were then used to conduct further analyses to investigate the relationship between these traits and scam victimisation and offending.

Factor	Internal Reliability	Items	Factor Loading
Unethical behaviour	.95	Used another person's debit/credit card without his/her permission.	0.81
		Used another person's licence/ID card without his/her permission	0.76
		Repeatedly contacted someone online even after they requested he/she to stop	0.78
		Repeatedly made sexual advances at someone	0.81
		Logged into another person's Facebook and posted a message	0.95
		Threatened another individual with violence online	0.85
		Logged into another person's email without his/her permission and sent an email	0.90
Impulsive behaviour	.82	I act on impulse	0.58
		I do things without thinking	0.52
		I am often distracted when thinking	0.49
		I say things without thinking	0.43
		I act on the spur of the moment	0.55
		I am less cautious about what I say online than about what I say in person	0.45
		I change hobbies	0.43
		I get easily bored when solving thought problems	0.49
		I buy things on impulse	0.59
		I spend or charge more than I earn	0.52

Online disinhibition	.88	I am more confident online than I am offline	0.47
		I am more outgoing online than I am offline	0.58
		I find communicating with others easier on the internet than in person	0.50
		I make friends more easily online than I do offline	0.55
		My behaviours online are less restricted than in person	0.52
		I say things on the internet that I would not say in person	0.52
		I act tougher on the internet than I do face to face	0.52
		I act differently online than I do offline	0.39
Personality traits	.72	I am a steady thinker	0.50
		I plan for job security	0.47
		I am dependable, self-disciplined	0.41
		I am future-oriented	0.50
		I plan tasks carefully	0.44
		I fidget at plays or lectures	0.40
		I plan trips well ahead of time	0.37
		I am restless at theatres or lectures	0.28
		I am a careful thinker	0.18

Linear Regressions

After obtaining our variables of interest from the EFA, we conducted regression analyses. A multinomial logistic regression was conducted for the dependent variable of scam victimisation as it has been employed in similar studies of crimes such as human trafficking (Twis, 2020). The majority of the participants have not fallen victim to a scam before (n = 90, 68.7%), a small number had nearly fallen for a scam (n = 9, 6.8%), while a small minority were scam victims (n = 3, 23.1%). We fitted a full model with the independent variables of (a) unethical behaviour (M = 1.06, SD = 0.30), (b) impulsive behaviour (M =2.29, SD = 0.49), (c) online disinhibition (M = 2.77, SD = 0.88), (d) personality traits (M = 3.10, SD = 0.39), (e) potential scam offending (M = 1.37, SD = 0.75), (f) detachment from victims (M = 1.44, SD = 0.86), and (g) gender. These variables accounted for 18.2% of the variance in scam victimisation and a goodness-of-fit tests revealed that the model does not significantly fit the data, χ^2 [7] = 12.81, p = .077. We experimented with several variations of independent variables to obtain a model that significantly fits our data. The derived model includes the independent variables of unethical behaviour, impulsivity, personality traits, detachment from victims, and gender, χ^2 [5] = 12.41, p = .030. These variables accounted for 17.7% of the variance in scam victimisation.

Only detachment from victims significantly predicted scam victimisation. Specifically, individuals who feel greater detachment from victims are more likely to have nearly fallen for a scam than not have fallen for a scam before (β = 57.489, p < .001).

A stepwise regression was conducted for the dependent variable of potential scam offending behaviour with the independent variables of (a) unethical behaviour, (b) impulsive behaviour, (c) online disinhibition, (d) personality traits, (e) scam victimisation, (f) detachment from victims, and (g) gender. The final model fitted only included the variables of (a) unethical behaviour, (b) impulsivity, (c) online disinhibition, and (d) detachment from victims. These variables accounted for 48.6% of the variance, and significantly predict potential scam offending behaviour (R^2 = .486, = F(7, 123) = 18.55, p < .001).

Unethical behaviour showed a positive relationship with potential scam offending (β = .632, p < .001). This indicates that individuals who perform unethical behaviours are more likely to be scammers. Impulsivity showed a positive relationship with potential scam offending as well (β = .295, p = .005). This shows that people who are impulsive are more likely to be scammers. Detachment from the victim was found to have a strong positive relationship with the likelihood of being a scammer (β = .515, p < .001). This suggests that individuals who feel detached from their victims are more likely to engage in scamming behaviour.

Lastly, we conducted another stepwise linear regression for the dependent variable of detachment from victims with the independent variables of (a) unethical behaviour, (b) impulsive behaviour, (c) online disinhibition, (d) personality traits, (e) potential scam offending, (f) scam victimisation, and (g) gender. The final model fitted only included the variables of (a) unethical behaviour, (b) online disinhibition, (c) gender, and (d) being a scammer. These variables accounted for 46.1% of the variance, and significantly predict detachment from victims ($R2$ = .464 = $F(7, 123)$ = 17.05, p < .001).

Unethical behaviour showed a negative relationship with detachment from victims (β = -.452, p = .025). This indicates that individuals who perform unethical behaviours are more likely to feel detached from victims. Online disinhibition showed a positive relationship with the likelihood of being detached from victims (β = .212, p = .002). This suggests that individuals who exhibit more online disinhibition are more likely to feel detached from their victims. Being male also significantly predicted detachment from victims (β = .276, p = .036), indicating that males are more likely to feel detached from victims. Potential scamming behaviour was also found to have a positive relationship with the likelihood of being detached from victims (β = .714, p < .001), suggesting that individuals who engage in scamming activities are more likely to feel detached from their victims.

DISCUSSION

Given previous literature on scam victimisation, this study was conducted to investigate the factors associated with scam victimisation, potential scam offending behaviour, and detachment from victims applicable to Singapore youths. The results revealed several significant findings that contribute to our understanding of these phenomena.

Scam Victimisation

Regarding scam victimisation, our multinomial logistic regression analysis showed that only detachment from victims significantly predicts scam victimisation while controlling for the variables of unethical behaviour, impulsivity, personality traits, and gender.

Specifically, individuals who feel greater detachment from victims are more likely to fall for a scam. We add to the existing literature, factors that contribute to susceptibility to scam victimisation, as – to the best of our knowledge – detachment from victims has not been previously demonstrated as a significant factor in this context. Moreover, our findings further reinforce the presence of a victim-offender overlap within the realm of scams, as we reveal common cognitive processes shared by both victims and offenders.

Feeling detached from victims can include the cognition of neutralisation (Orjiakor et al., 2022), which encompasses perceiving the victim as partially responsible for the crime, such as believing that they are gullible enough to fall for a scam. By attributing responsibility to the victim, individuals may develop a belief that they can protect themselves from victimisation by avoiding the same behaviours as the victim (Agnew, 1985). Alternatively, neutralisation can involve trivialising the offence, minimising the harm inflicted upon the victim. By downplaying the consequences of scams, individuals may experience reduced fear of falling victim to such schemes (Greenberg & Ruback, 1982). These perceptions can create a false sense of security (Agnew, 1985), leading individuals to be less vigilant and consequently more susceptible to falling for scams.

Surprisingly, our regression analysis reveals that potential scam offending and online disinhibition do not significantly contribute to scam victimisation, contradicting previous literature. We discuss alternative explanations for the lack of association. Firstly, our data shows that there is a significant correlation between unethical behaviour and potential scam offending. When we include unethical behaviour as a variable in our model,

the unique variance contributed by potential scam offending becomes too small to significantly predict scam victimisation. Alternatively, there may not be a victim-offender overlap as suggested by literature, where scam victims are unlikely to become scam offenders or vice versa. Rather, these two groups only share similar characteristics, such as performing unethical behaviours (Choi et al., 2019; Kaakinen et al., 2021) or being detached from victims (Orjiakor et al., 2022), without actually transitioning into the other role.

Similarly, online disinhibition and impulsivity are significantly correlated, thus reducing the unique contribution of online disinhibition in the regression model when impulsivity is included. While online disinhibition does stem from low self-control like impulsivity (Wang et al., 2023), it may manifest in behaviours that do not necessarily leave them vulnerable to scammers. For example, people with lower online disinhibition may tend to flame or cyberbully others online as they have lower self-control in recognising social cues (Voggeser et al., 2018). In other words, individuals with low online disinhibition may indeed engage more readily with unfamiliar material or people online but do not necessarily imply that they are disclosing personal information that could be harmful to themselves. On the other hand, impulsive individuals may carry out risky behaviours because they rarely consider potential consequences before acting (Holt et al., 2016; Schreck, 1999). Therefore, online disinhibition may not contribute to scam victimisation as corresponding behaviours may not increase susceptibility to scams.

Scam Offending Behaviour

In terms of potential scam offending behaviour, our stepwise regression analysis identified several significant predictors. Unethical behaviour is found to positively influence scamming behaviour, as we expected. Extorting money from a victim at their expense and one's own personal gain is arguably an unethical behaviour, thus reflecting this positive association. Then, what exactly pushes individuals to perform unethical behaviours? Ismail and colleagues (2023) propose several reasons for this. The most pronounced one is financial gain. The prospect of gaining economic profits quickly will surpass ethical limits, especially for individuals who are less hesitant in conducting minor yet unethical activities (e.g., using another person's social media account without permission). Another motivation is the perception that offenders do not have to face the consequences of scamming others. This can be due to perceived anonymity or the nature of complex legal systems and procedures that increases the difficulty of prosecution. For example, the question of whether banks or the government should be held accountable for scam victimisation. Moreover, peer influence plays a strong role in influencing unethical behaviour, even in online scams (Jegede et al., 2016). Having peers that encourage unethical behaviour can greatly influence one's willingness to participate in criminal activity. Lastly, vulnerabilities and loopholes that arise out of users' dependence on digital technologies can serve as an opportunity for scams. Thus, having an available target may tempt and push some individuals into becoming scammers.

Impulsivity has also been found to have a positive relationship with potential scam offending, indicating that individuals who exhibit impulsive tendencies are more likely to be involved in scamming. This supports current literature that there is a positive association between impulsivity and criminal behaviour (e.g., Carroll et al., 2006; Loeber et al., 2012). Together with the findings from the previous section, it also supports the theory that both victims and offenders share the common characteristic of impulsivity (Kersten & Jansen, 2016). Ong's (2022) study provides a deeper investigation of how impulsivity affects scammers' decisions. She suggests three precursors that allows impulsive individuals to decide on committing a scam more quickly, the first two being financial pressure and opportunity. Specifically, impulsive individuals make quicker decisions to commit scams when the opportunity and pressure is high, but take longer to deliberate when opportunity is high and pressure is low. Therefore, it is important for individuals to remain vigilant and avoid leaving opportunities for scammers. The final precursor is justification, which allows the perpetrator to feel more comfortable with their actions. Perpetrators might realise that their actions may be harmful to others but try to justify why it can be deemed morally acceptable instead. This process may happen before or after committing the offence.

Lastly, detachment from the victim has a strong positive relationship with the likelihood of being a scammer. This suggests that individuals who feel

detached from their victims are more likely to engage in scamming behaviour, further emphasising the role of neutralisation in scam offending (Orjiakor et al., 2022). Neutralisation is a highly influential factor in scam offending, to the extent that it can overcome parents' beliefs about law enforcement and initial resistance to their children's scam offending behaviour (Aborisade, 2022). This emphasises the importance of implementing interventions that focus on comprehending and addressing the psychological mechanisms underlying scamming behaviour. It is crucial to prevent the dissemination and endorsement of these cognitive processes among peers, particularly considering that peer subcultures can further promote scam offending (Jegede et al., 2016).

Detachment from Victims

Our analysis of detachment from victims reveals that unethical behaviour is negatively associated with detachment from victims, indicating that individuals who perform unethical behaviours are more likely to feel detached from victims. This finding is in line with how neutralisation cognitions justify unethical behaviours, as discussed in the previous sections.

Additionally, online disinhibition shows a positive relationship with detachment from victims, suggesting that individuals who exhibit more online disinhibition are more likely to feel detached from their victims. This finding may reflect the desensitisation and deindividuation effects of online environments, where individuals may perceive their actions as less impactful or consequential. In line with this proposition, flaming and cyberbullying behaviours that stem out of online disinhibition support this argument through lowered levels of empathy among these perpetrators (Wang et al., 2021, Wright & Wachs, 2019). Hence, our findings reveal that online disinhibition can encourage negative online behaviours, including scamming, possibly through its association with detachment from victims.

Lastly, being male significantly predicts detachment from victims, indicating that males are more likely to feel detached from victims. This gender difference in emotional detachment may be influenced by societal norms and expectations regarding masculinity and emotional expression (Bennett et al., 2005). More specifically, males' social cognitive development (e.g., perspective taking and empathetic understanding) may be less developed than females' due to later acquisition of these social skills. Additionally, empathy is more emphasised among females than males during their upbringing (Ross & Fabiano, 1985), thus contributing to males' emotional detachment from others.

CONCLUSION

Overall, these findings provide valuable insights into the factors associated with scam victimisation, potential scam offending behaviour, and detachment from victims. The results underscore the importance of considering individual characteristics, such as detachment and unethical behaviour, in understanding vulnerability to scams and engagement in scam-related activities. As our analyses are exploratory, it is important to interpret our findings with caution and consider them as preliminary until further confirmatory research is conducted. Future research can further examine the underlying mechanisms of scam victimisation and scam offending, and explore potential interventions to mitigate scam victimisation and scamming behaviour, with a focus on responsible online behaviour and highlighting vulnerabilities unique to youths.

ABOUT THE AUTHORS

Lee Yu Jing
is a psychologist at the Home Team Psychological Division, Ministry of Home Affairs, Singapore. She graduated with a Bachelor of Social Sciences from Nanyang Technological University. Currently, she supports research in the areas of offender and rehabilitation psychology, communication psychology, and resilience psychology.

Carolyn Misir
is a principal psychologist in the Operations and Forensic Psychology Branch (OFP) of the Police Psychological Services Department, which supports police operations, crime investigations, victim support and police intelligence through offence research and profiling projects, as well as direct consultations with units in high profile ongoing cases. Carolyn oversees the crime-related areas of the work in OFP, while concurrently building deep domain expertise and research in the areas of investigative and criminal psychology through her concurrent appointment at the Home Team Psychology Division of the Ministry of Home Affairs, Singapore.

Ken Chen
is a Senior Research Analyst in the Home Team Psychology Division, of the Ministry of Home Affairs, Singapore. He has a Masters in Information Studies from Nanyang Technological University. Some of his publications pertain to psychological vulnerability to misinformation, as well as leveraging AI to analyse different kinds of social issues. He was an editor of How to Prepare for the Next Pandemic: Behavioural Sciences Insights for Practitioners and Policymakers (2021). His research interests include societal polarisations, online misinformation, information operations, strategic communications, and natural language processing. Currently, he is pursuing his PhD at the Nanyang Technological University, researching the use of AI in misinformation detection.

REFERENCES

Aborisade, R. A. (2022). Internet scamming and the techniques of neutralization: Parents' excuses and justifications for children's involvement in online dating fraud in Nigeria. *International Annals of Criminology, 60*(2), 199-219. https://doi.org/10.1017/cri.2022.13

Agnew, R. S. (1985). Neutralizing the impact of crime. *Criminal Justice and Behavior, 12*(2), 221-239. https://doi.org/10.1177/0093854885012002005

Bennett, S., Farrington, D. P., & Huesmann, L. R. (2005). Explaining gender differences in crime and violence: The importance of social cognitive skills. *Aggression and Violent Behavior, 10*(3), 263-288. https://doi.org/10.1016/j.avb.2004.07.001

Bossler, A. M., & Holt, T. J. (2009). On-line activities, guardianship, and malware infection: An examination of routine activities theory. *International Journal of Cyber Criminology, 3*(1).

Burden, M. (2023). The cybercrime victim-offender overlap: Evaluating predictors for victims, offenders, victim-offenders, and those who are neither. *Victims & Offenders, 1-19*. https://doi.org/10.1080/15564886.2022.2159598

Carroll, A., Hemingway, F., Bower, J., Ashman, A., Houghton, S., & Durkin, K. (2006). Impulsivity in juvenile delinquency: Differences among early-onset, late-onset, and non-offenders. *Journal of Youth and Adolescence, 35*, 517-527. https://doi.org/10.1007/s10964-006-9053-6

Choi, K. S., Cho, S., & Lee, J. R. (2019). Impacts of online risky behaviors and cybersecurity management on cyberbullying and traditional bullying victimization among Korean youth: Application of cyber-routine activities theory with latent class analysis. Computers in Human Behavior, 100, 1-10. https://doi.org/10.1016/j.chb.2019.06.007

Chuang J. Y. (2021). Romance scams: Romantic imagery and transcranial direct current stimulation. *Frontiers in Psychiatry, 12*, 738874. https://doi.org/10.3389/fpsyt.2021.738874

Cross, C. (2018). (Mis)understanding the impact of online fraud: Implications for victim assistance schemes. *Victims & Offenders, 13*(6), 757-776. https://doi.org/10.1080/15564886.2018.1474154

DeLiema, M., Volker, J., & Worley, A. (2023). Consumer experiences with gift card payment scams: Causes, consequences, and implications for consumer protection. *Victims & Offenders, 18*(7), 1282-1310. https://doi.org/10.1080/15564886.2023.2244468

Duffield, G. M., & Grabosky, P. N. (2001). *The psychology of fraud. Trends & Issues in Crime and Criminal Justice, 199*, 1-6.

Global Anti Scam Alliance. (2024, January). *The Global State of Scams 2023*. Retrieved from https://www.gasa.org/_files/ugd/b63e7d_92ac212a168843219668d5a28510ce16.pdf

Global Anti Scam Alliance. (2024, January). *The Global State of Scams in Singapaore 2023*. Retrieved from https://www.gasa.org/_files/ugd/7bdaac_6c385beac3bb438fb471e021f7461323.pdf

Greenberg, M. S., & Ruback, R. B. (1982). *Social psychology of the criminal justice system*. Brooks/Cole Publishing Company.

Group-IB. (n.d.). *The Global State of Scams Report 2022*. https://www.group-ib.com/resources/research-hub/gasa-2022/

Hernández, M. P., Schoeps, K., Maganto, C., & Montoya-Castilla, I. (2021). The risk of sexual-erotic online behavior in adolescents–Which personality factors predict sexting and grooming victimization? *Computers in Human Behavior, 114*, 106569. https://doi.org/10.1016/j.chb.2020.106569

Holt, T. J., Bossler, A. M., Malinski, R., & May, D. C. (2016). Identifying predictors of unwanted online sexual conversations among youth using a low self-control and routine activity framework. *Journal of Contemporary Criminal Justice, 32*(2), 108-128. https://doi.org/10.1177/1043986215621376

Ismail, A. S., Mohamad Haniff, M. A. M., Md Radzi, M. N., & Mohamad Rosman, M. R. (2023). Inside the mind of cybercriminals: Investigating the influence of socioeconomic factors on the ethical decision-making of cybercriminals. *Proceedings of 1st Glocal Symposium on Information and Social Sciences (GSISS) 2023*, 34-42. http://doi.org/10.5281/zenodo.8180744

James, B. D., Boyle, P. A., & Bennett, D. A. (2014). Correlates of susceptibility to scams in older adults without dementia. *Journal of Elder Abuse & Neglect, 26*(2), 107–122. https://doi.org/10.1080/08946566.2013.821809

Jegede, A. E., Olowookere, E. I., & Elegbeleye, A. O. (2016). Youth identity, peer influence and internet crime participation in Nigeria: A reflection. *Ife PsychologIA: An International Journal, 24*(1), 37-47.

Kaakinen, M., Koivula, A., Savolainen, I., Sirola, A., Mikkola, M., Zych, I., ... & Oksanen, A. (2021). Online dating applications and risk of youth victimization: A lifestyle exposure perspective. *Aggressive Behavior, 47*(5), 530-543. https://doi.org/10.1002/ab.21968

Kaiser, H. F. (1974). An index of factorial simplicity. *Psychometrika, 39*(1), 31–36. https://doi.org/10.1007/BF02291575

Kamil, A. (2022, April 5). Youth form about half of all scam-related offenders arrested in Singapore: Shanmugam. *The Straits Times*. https://www.todayonline.com/singapore/youth-form-about-half-all-scam-related-offenders-arrested-singapore-shanmugam-1865081

Kelley, C. M., Hong, K. W., Mayhorn, C. B., & Murphy-Hill, E. (2012). Something smells phishy: Exploring definitions, consequences, and reactions to phishing. *Proceedings of the Human Factors and Ergonomics Society Annual Meeting, 56*(1), 2108-2112. https://doi.org/10.1177/1071181312561447

Kennison, S. M., & Chan-Tin, E. (2020). Taking risks with cybersecurity: Using knowledge and personal characteristics to predict self-reported cybersecurity behaviors. *Frontiers in Psychology, 11*, 546546. https://doi.org/10.3389/fpsyg.2020.546546

Kerstens, J., & Jansen, J. (2016). The victim–perpetrator overlap in financial cybercrime: Evidence and reflection on the overlap of youth's on-line victimization and perpetration. *Deviant Behavior, 37*(5), 585-600. https://doi.org/10.1080/01639625.2015.1060796

Kirwan, G. H., Fullwood, C., & Rooney, B. (2018). Risk factors for social networking site scam victimization among Malaysian students. *Cyberpsychology, Behavior, and Social Networking, 21*(2), 123-128. https://doi.org/10.1089/cyber.2016.0714

Klapatch, L., Hanoch, Y., Wood, S., & Hengerer, D. (2023). Consumers' response to mass market scam solicitations: profiling scams and responses. *Psychology, Crime & Law, 29*(9), 903-921. https://doi.org/10.1080/1068316X.2022.2038599

Kostić, J., Panić, T., & Pedović, I. (2016). Problematic online behaviors and experiences of adolescents: Correlations with parental mediation, information disclosure and personality characteristics. *British Journal of Education, Society & Behavioural Science, 18*(4), 1-14. https://doi.org/10.9734/BJESBS/2016/30251

Liau, A. K., Khoo, A., & Ang, P. H. (2008). Parental awareness and monitoring of adolescent Internet use. *Current Psychology, 27*, 217-233. https://doi.org/10.1007/s12144-008-9038-6

Loeber, R., Menting, B., Lynam, D. R., Moffitt, T. E., Stouthamer-Loeber, M., Stallings, R., ... & Pardini, D. (2012). Findings from the Pittsburgh Youth Study: Cognitive impulsivity and intelligence as predictors of the age–crime curve. *Journal of the American Academy of Child & Adolescent Psychiatry, 51*(11), 1136-1149. https://doi.org/10.1016/j.jaac.2012.08.019

Madden. (2017). *How technology experiences and resources vary by socioeconomic status, race, and ethnicity*. Data & Society. https://datasociety.net/library/privacy-security-and-digital-inequality/

Maddux, J. E. (2016). Self-efficacy. In S. Trusz & P. Bąbel (Eds.), *Interpersonal and intrapersonal expectancies* (pp. 41–46). Routledge/Taylor & Francis Group. https://doi.org/10.4324/9781315652535-5

Miró, F. (2014). Routine activity theory. In J. M. Miller (ed.), *The encyclopedia of theoretical criminology* (pp. 1-7). Wiley-Blackwell.

Mitchell, M. E., Lebow, J. R., Uribe, R., Grathouse, H., & Shoger, W. (2011). Internet use, happiness, social support and introversion: A more fine grained analysis of person variables and internet activity. *Computers in Human Behavior, 27*(5), 1857-1861. http://doi.org/10.1016/j.chb.2011.04.008

Modic, D., & Lea, S. E. (2012). *How neurotic are scam victims, really? The big five and Internet scams* [Conference presentation]. Conference of the International Confederation for the Advancement of Behavioral Economics and Economic Psychology, Exeter, United Kingdom. https://doi.org/10.2139/ssrn.2448130

Näsi, M., Oksanen, A., Keipi, T., & Räsänen, P. (2015). Cybercrime victimization among young people: A multi-nation study. *Journal of Scandinavian Studies in Criminology and Crime Prevention, 16*(2), 203-210. http://doi.org/10.1080/14043858.2015.1046640

Nguyen, A. L., Mosqueda, L., Windisch, N., Weissberger, G., Axelrod, J., & Han, S. D. (2021). Perceived types, causes, and consequences of financial exploitation: Narratives from older adults. *The Journals of Gerontology: Series B, 76*(5), 996-1004. https://doi.org/10.1093/geronb/gbab010

Ong, A. S. (2022). Think first, act later, or act first, think later: Does the fraud triangle hold when individuals are impulsive. *Journal of Forensic and Investigative Accounting, 14*(1), 11-38.

Orjiakor, C. T., Ndiwe, C. G., Anwanabasi, P., & Onyekachi, B. N. (2022). How do internet fraudsters think? A qualitative examination of pro-criminal attitudes and cognitions among internet fraudsters in Nigeria. *The Journal of Forensic Psychiatry & Psychology, 33*(3), 428-444. https://doi.org/10.1080/14789949.2022.2051583

Peluchette, J. V., Karl, K., Wood, C., & Williams, J. (2015). Cyberbullying victimization: Do victims' personality and risky social network behaviors contribute to the problem? *Computers in Human Behavior, 52*, 424-435. https://doi.org/10.1016/j.chb.2015.06.028

Petrosyan, A. (2024, May 2). *Average daily time spent using the internet by 4th quarter 2023, by age and gender*. Statista. https://www.statista.com/statistics/1378510/daily-time-spent-online-worldwide-by-age-and-gender/

Pituch, K. A., & Stevens, J. P. (2015). *Applied multivariate statistics for the social sciences: Analyses with SAS and IBM's SPSS* (6th ed.). Routledge. https://doi.org/10.4324/9781315814919

Rhoads, J. (2023). Psychological effects of cybercrime on minorities: Short-term and long-term impacts. *Journal of Empirical Social Science Studies, 7*(1), 1-31. https://doi.org/10.17613/xf5e-1r67

Ross, R. R., & Fabiano, E. (1985). *Time to think: A cognitive model of delinquency prevention and offender rehabilitation*. Institute of Social Sciences & Arts, Incorporated.

Şahin, C. (2011). An analysis of internet addiction levels of individuals according to various variables. Turkish Online *Journal of Educational Technology, 10*(4), 60-66.

Schouten, A. P., Valkenburg, P. M., & Peter, J. (2007). Precursors and underlying processes of adolescents' online self-disclosure: Developing and testing an "Internet-attribute-perception" model. *Media Psychology, 10*(2), 292-315. http://doi.org/10.1080/15213260701375686

Schreck, C. J. (1999). Criminal victimization and low self-control: An extension and test of a general theory of crime. *Justice Quarterly, 16*(3), 633-654. https://doi.org/10.1080/07418829900094291

Singapore Police Force. (2024a, February). *Annual Crime Brief 2023*. https://www.police.gov.sg/media-room/statistics

Singapore Police Force. (2024b, February). *Annual Scams and Cybercrime Brief 2023*. https://www.police.gov.sg/Media-Room/Statistics

Statista. (2023, May 10). *Overall crime rate in Singapore from 2012 to 2021*. https://www.statista.com/statistics/628339/crime-rates-in-singapore/

Suler, J. (2004). The Online disinhibition effect. *CyberPsychology & Behavior, 7*(3), 321–326. https://doi.org/10.1089/1094931041291295

Towner, E., Grint, J., Levy, T., Blakemore, S. J., & Tomova, L. (2022). Revealing the self in a digital world: A systematic review of adolescent online and offline self-disclosure. *Current Opinion in Psychology, 45*, 101309. https://doi.org/10.1016/j.copsyc.2022.101309

Twis, M. K. (2020). Predicting different types of victim-trafficker relationships: A multinomial logistic regression analysis. *Journal of Human Trafficking, 6*(4), 450-466. https://doi.org/10.1080/23322705.2019.1634963

University of Twente. (2022, March 29). *One in six Dutch citizens falls victim to fraudsters*. https://www.utwente.nl/en/research/themes/digital/news/2022/3/525876/one-in-six-dutch-citizens-falls-victim-to-fraudsters

van de Weijer, S. G., & Leukfeldt, E. R. (2017). Big five personality traits of cybercrime victims. *Cyberpsychology, Behavior, and Social Networking, 20*(7), 407-412. https://doi.org/10.1089/cyber.2017.0028

Varga, G. (n.d.). *The Gen-Z fraud report: Young Americans & fraud*. Seon. https://seon.io/resources/gen-z-report-online-fraud/

Voggeser, B. J., Singh, R. K., & Göritz, A. S. (2018). Self-control in online discussions: Disinhibited online behavior as a failure to recognize social cues. *Frontiers in Psychology, 8*, 2372. https://doi.org/10.3389%2Ffpsyg.2017.02372

Wang, C. (2022). Online dating scam victims psychological impact analysis. *Journal of Education, Humanities and Social Sciences, 4*, 149-154. http://dx.doi.org/10.54097/ehss.v4i.2740

Wang, L., Jiang, S., Zhou, Z., Fei, W., & Wang, W. (2023). Online disinhibition and adolescent cyberbullying: A systematic review. *Children and Youth Services Review, 156*, 107352. https://doi.org/10.1016/j.childyouth.2023.107352

Wang, X., Qiao, Y., Li, W., & Dong, W. (2022). How is online disinhibition related to adolescents' cyberbullying perpetration? Empathy and gender as moderators. *The Journal of Early Adolescence, 42*(5), 704-732. https://doi.org/10.1177/02724316211064515

Whitty, M. T., & Buchanan, T. (2016). The online dating romance scam: The psychological impact on victims – both financial and non-financial. *Criminology & Criminal Justice, 16*(2), 176–194. https://doi.org/10.1177/1748895815603773

Wright, M. F., & Wachs, S. (2021). Does empathy and toxic online disinhibition moderate the longitudinal association between witnessing and perpetrating homophobic cyberbullying? *International Journal of Bullying Prevention, 3*, 66-74. https://doi.org/10.1007/s42380-019-000

Ybarra, M. L., & Mitchell, K. J. (2008). How risky are social networking sites? A comparison of places online where youth sexual solicitation and harassment occurs. *Pediatrics, 121*(2), e350-e357. https://doi.org/10.1542/peds.2007-0693

Zia, A., & Malik, A. A. (2019). Usage of social media, age, introversion and narcissism: A correlational study. *Bahria Journal of Professional Psychology, 18*(2), 33-54.

ABETTING SCAMMERS FOR A QUICK BUCK?
A SURVEY OF SINGAPOREAN YOUTHS' INVOLVEMENT IN ILLICIT SCAM-RELATED ACTIVITIES

Clarissa Foo, Kwek Boon Siang, Stephanie Chan, Chen Yongjie & Wong Jia Wen
Home Team Psychology Division, Ministry of Home Affairs, Singapore

ABSTRACT

Locally and internationally, there have been increasing reports of youths being recruited for illicit activities that support the operations of scam syndicates, such as money muling or the selling of bank accounts. A convenience sample of almost 400 Singaporean youths aged 16 to 25 was surveyed to understand the scale and nature of their experiences with scam-related activities. The survey found that about half of the sampled youths received recruitment offers for illicit scam-related activities, about a quarter of whom subsequently participated in them. Additionally, recruitment offers that originated from a known associate were four times more effective in recruiting participants than online, anonymous ones, demonstrating the power of antisocial influence in the recruitment for scam-related activities. Finally, the article highlights key criminal attitudes and thinking associated with involvement in scam-related activities. Implications and recommendations for policy and public education are also discussed.

THE RISE OF YOUTH MONEY MULES

Internationally, there have been increasing reports of youths involved in illicit financial activities. For instance, the United Kingdom experienced a significant surge in the number of youth money mules between 2020 and 2021, with a 78% increase among those under 21, and a 76% increase among those aged 21 to 30 (Cifas, 2021; see Figure 1).

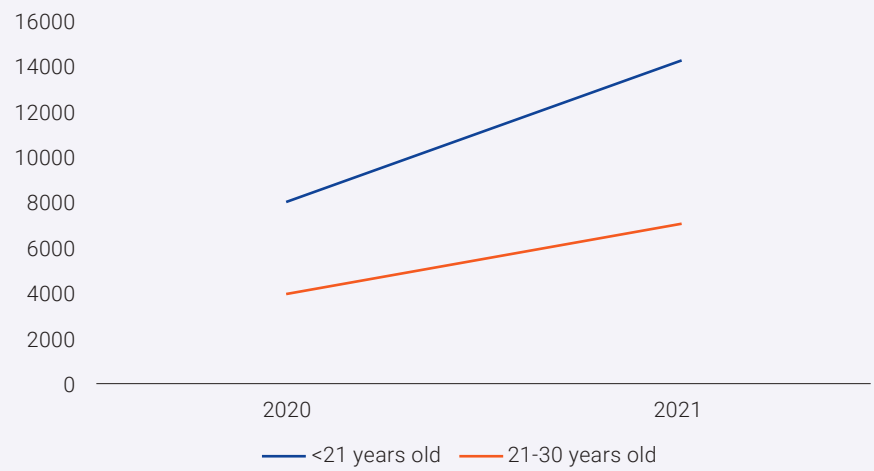


Figure 1. Number of Young Money Mules Identified in the United Kingdom

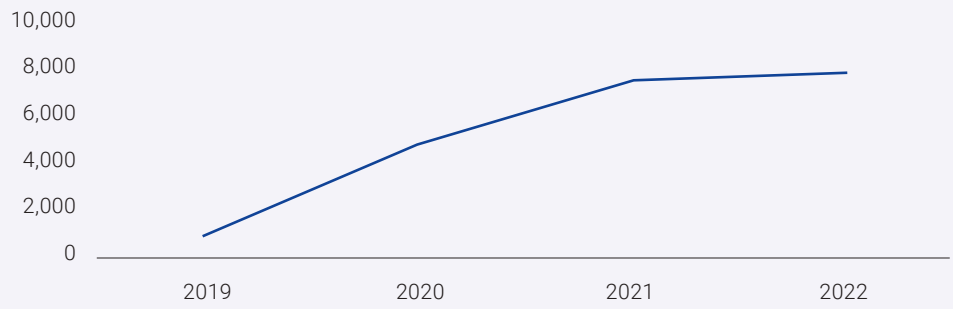


Figure 2. Number of Money Mules Arrested in Singapore between 2019 and 2022

A similar trend has been observed in Singapore. Between 2019 and 2022, local money mule arrests shot up by 680% (Hamzah, 2023; see Figure 2). Notably, 45% of money mule cases reported to the police between 2020 and 2022 involved individuals 25 years or younger (Tan, 2023).

These illicit financial activities often have ties to scam syndicates (Ministry of Home Affairs, 2022). Scam syndicates may launder their fraudulent proceeds through a complex network of money mules to conceal their illegitimate origin and avoid detection (Raza et al., 2020). To facilitate this, money mules typically receive and transfer these ill-gotten funds in and out of their personal bank accounts in exchange for a commission (Arevalo, 2015). Other mules may be tasked to sell their bank accounts or open several bank accounts at the behest of scam syndicates. Overall, while money mules may not be directly involved in scam operations, they are accomplices in the money laundering process.

While some money mules, like Irfan, are aware of the illegal nature of the activity, there are other unwitting mules who are tricked or pressured into moving ill-gotten funds (Arevalo, 2015). For example, syndicates may recruit unwitting mules online under the guise of a legitimate job opportunity (Dunham, 2006). Others, such as Lisa, may become mules under intimidation.

Irfan, 16

Irfan had just dropped out of the Institute of Technical Education when he heard that he could earn money by opening bank accounts for others to use for online gambling. He was reeled in by his secondary school friends who were in the "business". They said he could either get a one-time payment of $400 by selling an account, or a monthly payout of $150 by leasing it.

A friend gave him $1,000 to open two bank accounts, and a SIM card with a new number to register the accounts. All Irfan had to do was to meet his friend at a shopping mall, where he was coached on what to tell the bank staff. Following which, he sold one UOB account, and leased an OCBC account to his friend, making $850 in three months.

Then, he started receiving bank statements in the mail, including one which was 60 pages long. It showed transactions from strangers, including transfers of up to $80,000. He was afraid that the scam syndicates' criminal operations would all lead back to him. Sure enough, his bank accounts were frozen two months later. He was investigated by the police the following year (Tan, 2023).

Lisa, 21

Lisa's ordeal began in 2020 when she sought to borrow money from online loan services to cope with dire financial circumstances. Through a registration process, she was instructed to provide copies of her pay slips and identification cards. Thereafter, she was introduced extra fees, and her refusal to pay them led to relentless harassment and threats from the moneylender. Under immense pressure, Lisa used up her savings to cover the fees, enduring this situation for a year until January 2021. During this time, she was approached by multiple loan sharks, leading her to suspect that her personal details were used to borrow money from other illegal moneylenders, hence multiplying her debts and intensifying threats to her family.

Two months later, a loan shark presented Lisa with what seemed like a miraculous solution. For every ATM card she gives up, she can earn $300 per month. Tempted by the prospect of some financial relief, Lisa surrendered three ATM cards, only to not receive any compensation as promised. To make matters worse, the loan sharks promptly changed her account credentials, locking her out of her own accounts. Eventually, Lisa received a letter from the Police in 2022, suspecting her involvement in money laundering activities (Aqil, 2022).

Beyond traditional money muling, scam syndicates are also known to offer financial rewards in exchange for other activities that support their operations. Singpass credentials have also been bought by scam syndicates for the purposes of setting up new bank accounts to support money laundering operations (Lim, 2024). Furthermore, scam syndicates may fraudulently purchase mobile phone lines, social media accounts, and gaming accounts, which are subsequently used to contact a greater number of potential scam victims (Ministry of Home Affairs, 2024).

This article will use the umbrella term of illicit scam-related activities to refer to the wide array of illegal activities adopted by scam syndicates to facilitate their criminal operations. However, as the illicit scam-related activity of money muling is the most established in academic literature, much of the empirical evidence discussed in the following section is derived from research on money mules.

YOUTHS AS ATTRACTIVE TARGETS FOR SCAM SYNDICATES

There has been a significant increase in the number of youths involved in illicit scam-related activities (Kamil, 2022). Researchers have further identified youth vulnerabilities that may be readily exploited by scam syndicates, making them a particularly attractive recruitment target for illicit activities. These vulnerabilities include a) financial strain and materialistic attitudes, b) susceptibility to social influence and manipulation, and c) a lack of awareness about illicit scam-related activities and its impacts.

Financial Strain and Materialistic Attitudes

One of the most compelling motivations to participate in illicit scam-related activities in exchange for quick and easy money is perceived financial difficulty (Arevalo, 2015). Across the globe, young adults face greater financial difficulty due to a significant increase in costs of living and a poor economic outlook (Broom, 2023). In a global survey of 14,483 Gen Zs aged between 19 to 29 years old, 56% reported living paycheck to paycheck, while 45% took on side jobs to relieve financial pressures (Deloitte, 2024). Locally, 52% of 1,000 Singaporean youths aged 18 to 35 cited increasing costs of living as a key mental health stressor (Low, 2022). Hence, financial and mental health strains may create a sense of desperation and urgency, leaving many youths more vulnerable to the lure of fraudulent schemes that promise immediate financial relief.

Paradoxically, these financial trends come on the heels of increasingly materialistic attitudes among youths (Zawadzka et al., 2022). The prevalent and consistent consumption of social media has exposed youths to the lifestyles of wealthy individuals, resulting in unhealthy social comparisons and materialistic goals (Hu et al., 2023). Bekkers et al. (2022) found that Dutch youths aged between 18 to 25 were more

likely to engage with money mule recruitment advertisements on Instagram if its messaging had an emphasis on a luxurious lifestyle (e.g., "you will soon have a few thousand!"), compared to if it possessed neutralisation messaging (e.g., "it is completely legal!"). Hence, this suggests that materialistic attitudes and goals among youths may be a driver for recruitment into illicit scam-related activities. Taken together, widespread financial strain and materialistic attitudes work in tandem to leave youths vulnerable to involvement in such illicit activities.

Susceptibility to Social Influence and Manipulation

Due to their younger age, youths may be more suggestible, which leaves them more susceptible to social influence and manipulation. In the same experiment conducted by Bekkers et al. (2022), it was observed that money mule recruitment advertisements featuring messages that normalise money muling (e.g., "others did it before you!") worked well as a persuasion strategy. Furthermore, repeated exposure to such social media advertisements resulted in increased user engagement (i.e. higher click-through rate). This suggests that frequently receiving recruitment offers could create a perception that it is normal and socially acceptable to be involved in illicit scam-related activities (Bekkers et al., 2022). These effects are even more pronounced when recruitment offers originate from peers (Orjiakor et al., 2022). Antisocial peers may flaunt the wealth and gains derived from their own involvement in illicit activities, giving rise to tacit social influence and pressure that further entices vulnerable youths.

Susceptibility to social influence and manipulation not only makes youths more vulnerable to illicit recruitment offers, but it also renders them more compliant to criminal instructions (Arevalo, 2015). The compliance of youth money mules with criminal instructions has also been reported, with some individuals succumbing to pressure from the recruiters (Leukfeldt & Kleemans, 2019). These findings emphasise the influence of persuasion techniques and the potential impact of repeated and peer exposure on the decision-making processes of youths.

Lack of Awareness of Illicit Scam-Related Activities and their Impacts

A survey conducted of students aged 18 to 24 years in the United Kingdom found that 57% were unaware that money muling may be associated with the laundering of funds defrauded by scam syndicates (Pedro, 2022). This lack of awareness could explain why many youth money mules may mistake these lucrative recruitment offers as legitimate job opportunities (Leukfeldt & Kleemans, 2019; Vedamanikam & Chethiyar, 2020).

Even among youths who understand the criminal nature of scam-related activities, some may underestimate the consequences of money muling, such as its impact on scam victims (Bekkers et al., 2023; Orjiakor et al., 2022). Additionally, they may overestimate their ability to get away with the crime while underestimating the consequences if caught, thus signalling a sense of infallibility and optimism bias that youths may be more vulnerable to. Arevalo (2015) also argued that youths may be more geared towards instant gratification, which spurs them to focus on the short-term goal of quick cash, rather than the potential penalties, such as being barred from important loans in the future. Hence, it is not surprising that 43% of a sample of Irish youths aged 18 to 24 reported being either likely or very likely to use their own bank account to transfer money on behalf of someone else in exchange for a commission (Pickles, 2021).

RECRUITMENT TECHNIQUES

To recruit youths into illicit scam-related activities, scam syndicates rely on two main techniques: the use of social networks and online recruitment advertisements (Leukfeldt & Kleemans, 2019).

Social Network Recruitment

Similar to traditional crimes, social ties and antisocial influence continue to hold significance within cyber-criminal networks (Bekkers & Leukfeldt, 2023). In the Netherlands, an analysis of investigations into 14 cyber-criminal networks, which consisted of 211 money mules, found that 13 of them relied on recruitment via social networks (Leukfeldt & Kleemans, 2019). Existing members of the organised crime networks would approach social contacts

from their neighbourhoods, schools, or sports clubs with opportunities to earn quick cash. Individuals recruited through such means tend to be aware of the criminal nature of the activity, but choose to participate for monetary incentives (Arevalo, 2015). Social network recruitment is effective as individuals tend to feel pressured to comply with requests that come from family members or friends or participate to fit in with their peer groups (Bekkers et al., 2023).

Scam syndicates may even introduce referral schemes to incentivise existing syndicate members to recruit new members. Police investigations in Singapore have uncovered cases where existing syndicate members were instructed to invite more members to elevate their membership status, which would enable them to undertake more tasks for additional commissions (Singapore Police Force, 2022). Taken together, highly motivated syndicate members seem to leverage social relationships with their contacts to effectively recruit new individuals into illicit scam-related activities.

Online Advertisement Recruitment

On top of traditional social network recruitment, there is also a rising trend of online, anonymous recruitment into illicit scam-related activities via job portals and social media platforms (Arevalo, 2015). Under the guise of a legitimate job opportunity, individuals may become unwitting participants of illicit scam-related activities. As part of the "job", they may be tasked to move funds between various accounts under vague titles, such as "account manager", "money transfer agent", or "financial manager" (Dunham, 2006).

To reel in unsuspecting individuals for such "jobs", scam syndicates may rely on get-rich-quick schemes, which feature job advertisements with minimal or unclear work requirements, coupled with promises of disproportionately lucrative incomes (Bekkers et al., 2022; Rani et al., 2023; Raza et al., 2020). For example, a Malaysian national came across a job listing for a vague business development role based in Cambodia, offering an attractive monthly salary of RM5,000 to RM10,000 (see Figure 3; Channel News Asia, 2023). The advertisement also promised bonuses, food, accommodation, and flight tickets for international applicants.

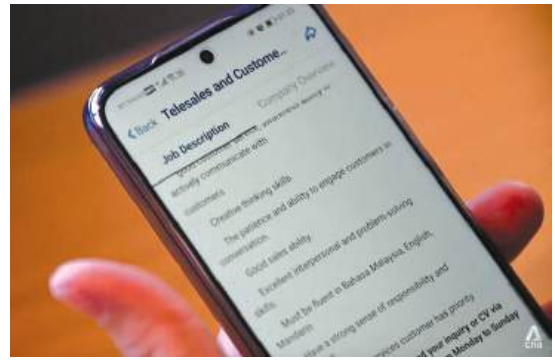


Figure 3. A Job advertisement under a Get-Rich-Quick Scheme

Get-rich-quick schemes are often used by scam syndicates to attract and identify youths interested in earning quick and easy money (Pickles, 2021; Shane, 2023; Vedamanikam & Chethiyar, 2020). According to a study conducted by Barclays (2019), 57% of university students were interested in job advertisements that did not require any prior experience, while 50% were attracted by work-from-home job offers promising quick and easy money. This provides some evidence that get-rich-quick schemes may be effective in recruiting youths.

Scam syndicates may also rely on illusion-of-choice schemes to appeal to youths' desire for quick and easy money. In an illusion-of-choice scheme, scam syndicates often present individuals with multiple job offerings, each promising attractive returns. These jobs may entail giving up one's personal information like bank account PINs, ATM cards, Singpass credentials and more (Aqil, 2022; Bekkers et al., 2022; Ministry of Home Affairs, 2022; Raza et al., 2020). Multiple job offerings provide individuals with a false sense of choice and control, ultimately driving them to apply for illicit recruitment offers disguised as legitimate job offers.

Compared to job portal recruitment advertisements, those on social media tend to be more forward about the illicit nature of the scam-related activity. An experiment by FinTrail (2020) found that popular social media platforms such as Instagram, Facebook, and X (previously known as Twitter) had accounts or posts related to money muling. Additionally, a survey discovered that 57% of Dutch youths encountered money mule recruitment advertisements on social media platforms, such as Instagram and Snapchat

(Bekkers et al., 2023). Locally, there have been many reports of illicit recruitment advertisements on Telegram, a messaging app that is extremely popular among Singapore youths (Hamzah, 2023). Some of these advertisements do not attempt to conceal the illicit nature of the request, using terminology like "clean" to refer to bank or Singpass accounts that have not been previously implicated in criminal activities (see Figure 4). The commissions that individuals stand to earn from selling their bank account or Singpass credentials are also clearly stated.

Figure 4. Illicit Recruitment Advertisements Broadcast on Telegram

LEGISLATIVE MEASURES AGAINST ILLICIT SCAM-RELATED ACTIVITIES

To clamp down on participation in various illicit scam-related activities, several legislative measures have been introduced in Singapore. These measures provide law enforcement officials with an expanded toolkit to act against individuals who participate in various illicit scam-related activities, such as money muling, the disclosure of banking or Singpass credentials, and the handing over of SIM cards to syndicates (see Figure 5).

To raise public awareness of illicit scam-related activities and relevant legislative amendments, a comprehensive public education campaign has been rolled out by the Singapore Police Force (SPF) and National Crime Prevention Council (NCPC). The campaign reminds the public that payment accounts, Singpass accounts, and mobile phone lines are for personal use only. Should these accounts or phone lines be used by or at the behest of others, individuals may be held criminally liable (see Figure 6 on next page).

Bill	Offence	Penalties
Corruption, Drug Trafficking and Other Serious Crimes Act	Rash money laundering: carrying out a suspicious transaction while failing to make further queries to address suspicions.	A fine of up to $250,000 or imprisonment of up to five years, or both.
	Negligent money laundering: carrying out a transaction despite the presence of red flags or suspicious indicators.	A fine of up to $150,000 or imprisonment of up to three years, or both.
	Allowing another person to access, operate, or control one's payment account.	A fine of up to $50,000 or imprisonment of up to three years, or both.
Computer Misuse Act	Disclosing one's Singpass credentials to another person.	A fine of up to $10,000 or imprisonment of up to three years, or both.
Law Enforcement and Other Matters Bill	Handing over one's local SIM cards to another person or allowing particulars to be used to sign up for a local SIM card by another person.	A fine of up to $10,000 or imprisonment of up to three years, or both.

Figure 5. Summary of Legislative Measures Against Participation in Scam-related Activities

Figure 6. Public Education Poster on Legislative Amendments

THE CURRENT STUDY

While legislation has made significant strides against scam-related activities, there is still a lack of research in this area, especially with local youths. This is concerning, given that youths are a vulnerable population that make up a large proportion of those arrested (Tan, 2023). To address the research gap, the Home Team Psychology Division (HTPD) conducted an exploratory survey with almost 400 Singaporean youths to explore the scale and nature of the issue locally. Specifically, the survey focused on 5 key themes:

1. Receiving Recruitment Offers for Illicit Scam-Related Activities
   a. What proportion of youths encountered recruitment offers for scam-related activities?
   b. What demographic factors increased or decreased youths' risk of encountering such recruitment offers?
2. Responding to Recruitment Offers for Illicit Scam-Related Activities
   a. What proportion of youths participated in illicit scam-related activities?
   b. What demographic factors increased or decreased youths' risk of participating in such activities?
3. Sources of Recruitment Offers for Illicit Scam-Related Activities
   a. What were the sources of recruitment offers (e.g., online ads, or friends)?
   b. Which sources increased or decreased youths' risk of participating in such activities?
4. Motivations for (Not Accepting) Recruitment Offers
   a. What were the motivations for youths to participate in illicit scam-related activities?
   b. What were the motivations for youths who chose not to participate in illicit scam-related activities?
5. Anti-Scam Behaviours and Exposure to Recruitment Offers
   a. What anti-scam behaviours do youths engage in?
   b. What is the link between youths' anti-scam behaviours and their exposure to recruitment offers for illicit scam-related activities?

METHODS

Participants

Convenience and snowball sampling was conducted among 800 youth participants of the Criminal Behavioural Analysis Competition (CBAC) 2023, a crime-solving competition organised by the Home Team Psychology Division (HTPD), Scam Public Education Office (SPEO), and the National Crime Prevention Council (NCPC).[1] In total, 390 participants completed the survey. They were automatically entered into a lucky draw where they stood a chance to win a SGD $5 Grab voucher.

[1] As a result of convenience and snowball sampling, the sample was not nationally representative and findings from the survey are not generalisable to all Singaporean youths. Furthermore, youths in the sample took part in a government-affiliated crime-solving competition. Hence, insights derived from their data may paint a more positive picture of Singaporean youths' involvement in illicit scam-related activities.

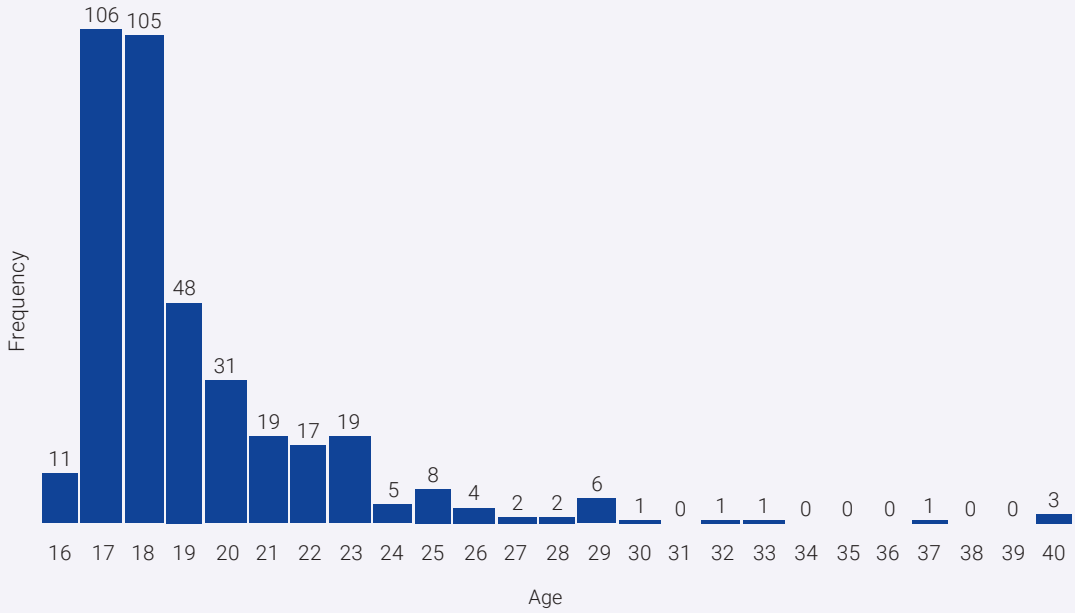


Figure 7. Age Distribution of Survey Participants

Participants' ages ranged from 16 to 40 years (*M* = 19.41, *SD* = 3.49; see Figure 7). Although a small minority of 5.1% (*n* = 20) were older than the typical age range for youths (i.e., above 25 years of age), their responses did not adversely affect the results and were retained for analysis.

The sample consisted of 63.9% (*n* = 250) females, and 17.4% (*n* = 68) were previously victims of scams. Since most of the participants belonged to local Junior Colleges (26.3%; *n* = 103), Polytechnics (43.4%; *n* = 170), and Universities (26.1%; *n* = 117), subsequent educational level analyses compared these groups (see Figure 8).

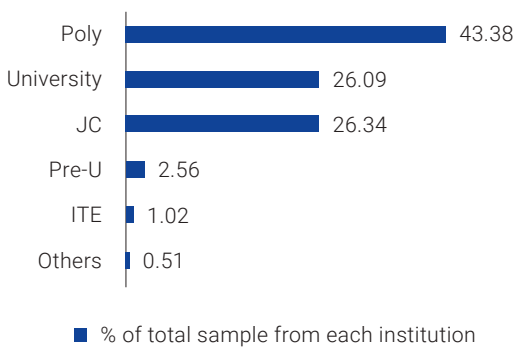


Figure 8. Breakdown of Participants' Educational Institution

Procedure

Survey participants were invited to complete the survey online. Before proceeding to the survey questions, participants were briefed on the survey and were informed of its anonymous nature. Next, their consent was sought before they answered basic demographic questions, such as their age, gender, educational institution, and scam victimisation history.

Participants were asked to provide their responses to the following three sections in the survey, which were aligned with the research questions:

a. Recruitment and Involvement in Illicit Scam-Related Activities
b. Attitudes towards Illicit Scam-Related Activities
c. Take-Up and Frequency of Anti-Scam Behaviours

Survey Design and Materials

Survey Section A: Recruitment and Involvement in Illicit Scam-Related Activities

Participants were presented with a list of 13 illicit scam-related activities that were developed by the researchers based on literature review and consultation with police officers who specialise in scams investigations (e.g., opening a bank

account and giving someone else control of it). Participants were asked to indicate if they were ever offered a commission for completing each of the thirteen activities.

If they indicated receiving such offers for at least one of the 13 activities, participants were then asked to indicate which recruitment channels the various recruitment offers originated from (e.g. online advertisements). Next, from a list of activities they received recruitment offers for, participants were asked to indicate which of them they participated in.

Survey Section B: Attitudes towards Illicit Scam-Related Activities

Participants who had received at least one recruitment offer for an illicit scam-related activity were then surveyed on their attitudes towards participation in such activities. Specifically, those who indicated that they took up recruitment offers were asked to endorse up to five (out of a list of 14) pro-criminal attitudes that explained their involvement in such activities (e.g., "I thought the activity was harmless to others"). The list of pro-criminal attitudes was derived from extant literature on differential association theory, rational choice theory, and social cognitive theory (Casey et al., 2013).

Similarly, participants who indicated that they rejected recruitment offers were asked to choose up to five (out of a list of 14) anti-criminal attitudes that guided their decision-making (e.g., "I thought it would cause harm to others"). The list of anti-criminal attitudes was derived through reversed phrasing of the list of pro-criminal attitudes.

Survey Section C: Take-Up and Frequency of Anti-Scam Behaviours

Finally, the take-up and frequency of anti-scam behaviours was measured to investigate if such behaviours would protect against exposure to recruitment offers. All survey participants indicated whether they engaged in a list of three anti-scam behaviours adapted from the Scam Public Education Office (SPEO) Dipstick Survey 2023 (e.g., "I installed the ScamShield app to my mobile phone").

Finally, all survey participants rated on a scale of 1 (never) to 5 (always) how frequently they engaged in a list of anti-scam behaviours (e.g., "Report numbers which I suspect to be attempting to scam me via my mobile phone or communication apps"). These anti-scam behaviours were adapted from the National Prevalence Survey of Scams 2020 conducted by the Home Team Psychology Division (HTPD), formerly known as the Home Team Behavioural Sciences Centre (HTBSC; 2020).

RESULTS

Key Finding 1: One in two youths received recruitment offers to take part in illicit scam-related activities.

Among the participants, 53.3% (n = 208) received at least one recruitment offer to participate in an illicit scam-related activity (see Figure 9). Out of those who received recruitment offers, about a third (36.1%) of them received more than two recruitment offers (see Figure 10).

Figure 9. Proportion of Youths who Received Recruitment Offers

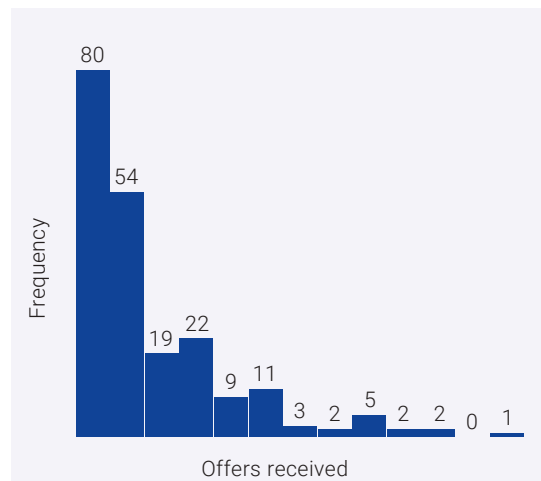


Figure 10. Histogram of the Number of Recruitment Offers Received

**Participants could report receiving multiple offers. Hence, total offers is greater than the sample size.*

Figure 11. Breakdown of Recruitment Offers Received

The most common illicit scam-related activities that participants received recruitment offers for were related to money muling (e.g., working as a "Money Transfer Agent" or transferring money in and out of one's bank account; see Figure 11). Communications-related activities, such as giving up control of one's social media or gaming account or posting fraudulent reviews of e-commerce products were the second most common.

Key Finding 2: Scam victims, males, and younger youths were more likely to receive recruitment offers to take part in illicit scam-related activities.

A chi-square test of independence revealed that compared to those who had not previously fallen for scams (evaders), scam victims were significantly more likely to receive recruitment offers for illicit scam-related activities, χ^2 (1, n = 390) = 4.9, p = 0.03 (see Figure 12). Furthermore, an Analysis of Variance (ANOVA) revealed that on average, scam victims received a greater number of recruitment offers compared to scam evaders, at a magnitude which approached significance, F (1, 388) = 3.71, p = 0.06, η^2 = 0.009 (see Figure 13).

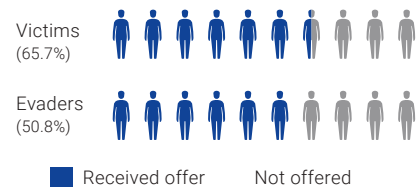


Figure 12. Proportion of Scam Victims and Evaders that Received Offers

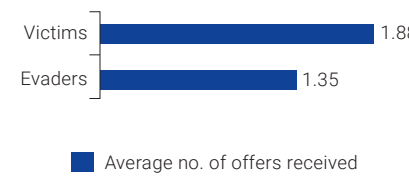


Figure 13. Average Number of Recruitment Offers Received by Scam Victims and Evaders

A regression analysis indicated that age negatively predicted the number of recruitment offers received by participants, R^2 = 0.02, F(1, 388) = 48.9, p = 0.003. In other words, younger participants tended to receive more recruitment offers (see Figure 14). However, there were no significant differences in the receiving of recruitment offers between educational groups, which included students of varying age ranges.

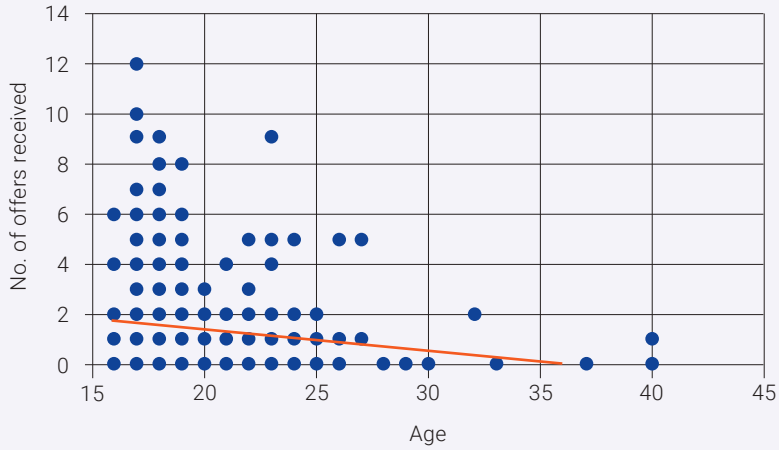


Figure 14. Number of Recruitment Offers Received by Age

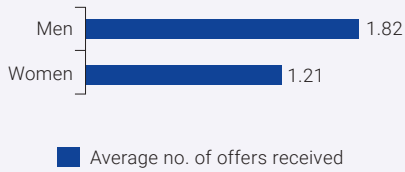


Figure 15. Average Number of Recruitment Offers Received by Men and Women

Finally, an ANOVA revealed that men received a significantly higher number of offers compared to women, F (1, 375) = 7.2, p = 0.007, η^2 = 0.02 (see Figure 15).

Key Finding 3: One in four youths accepted recruitment offers for illicit scam-related activities.

Of participants who received recruitment offers, 26.0% (n = 54) accepted such offers and partook in illicit scam-related activities (13.9% of the total sample; see Figure 16). Most of these youths (83.3%) were involved in one to two scam-related activities each (see Figure 17).

Similar to recruitment offers, banking and communications activities were common, with money muling being the most common illicit scam-related activity (see Figure 18).

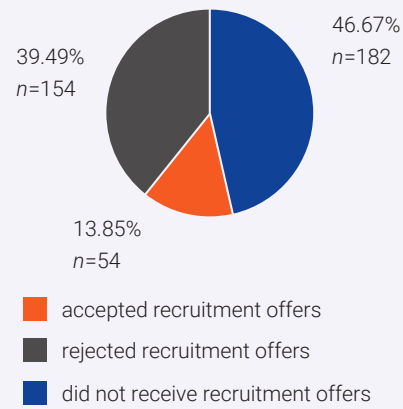


Figure 16. Proportion of Youths that Participated in Scam-Related Activities

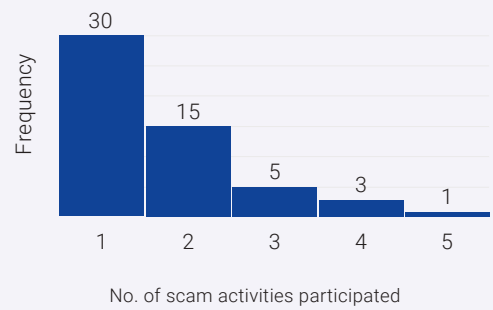
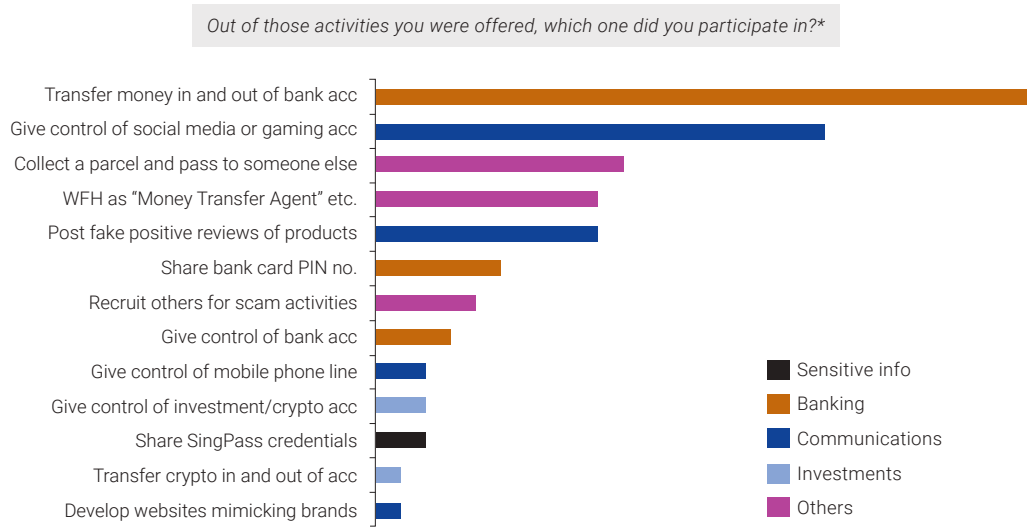


Figure 17. Histogram of the Number of Scam-Related Activities Parcitipated In



*Participants could report participating in more than one activity. Hence, total participation is greater than the sample size.

Figure 18. Breakdown of Participation in Scam-Related Activities

Key Finding 4: Polytechnic students were three times more likely to accept recruitment offers compared to Junior College and University students.

An ANOVA revealed that Polytechnic students were significantly more likely to accept recruitment offers compared to those from Junior College, X^2 (1, N = 148) = 14.4, p < 0.001 (see Figure 19). Furthermore, Polytechnic students, compared to Junior College students, participated in a significantly greater number of illicit scam-related activities on average, F (1, 146) = 15.8, p < 0.001, η^2 = 0.1 (see Figure 20).

Similarly, a chi-square analysis revealed that Polytechnic students were significantly more likely to accept such offers compared to University students, χ^2 (1, *N* = 138) = 5.0, *p* = 0.03. On average, Polytechnic students also accepted significantly more recruitment offers than their University counterparts, *F* (1, 136) = 8.1, *p* = 0.005, η^2 = 0.06.

Figure 19. Proportion of Students from Each Institution that Accepted or Rejected Offers

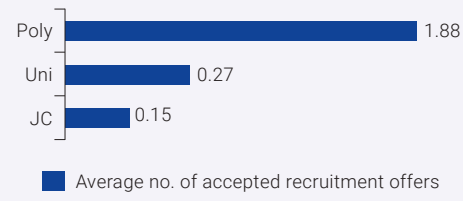


Figure 20. Average Number of Accepted Recruitment Offers by Institution

Key Finding 5: While anonymous online recruitment offers were far more common than those that originated from a known associate, the latter was four times more effective at recruiting youths.

The majority (76.0%) of recruitment offers originated from online strangers (i.e., strangers who approached via asynchronous messaging platforms such as WhatsApp) or online recruitment advertisements (see Figure 21). An ANOVA revealed that compared to Junior College and University students, Polytechnic students received significantly more offers from family members, friends, and other associates, F (2, 372) = 4.31, p = 0.014, η^2 = 0.023 (see Figure 22).

Overall, while online recruitment methods were more common, they were less effective at successfully recruiting individuals into illicit scam-related activities. Online recruitment offers were accepted at a rate of 14.4%, while 66.2% of those that originated from social networks were accepted.

Figure 21. Number of Recruitment Offers Oriignating from Various Recruitment Sources

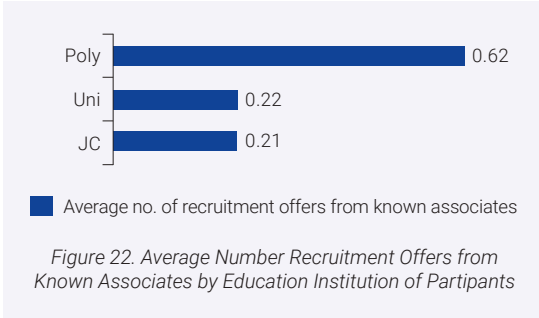


Figure 22. Average Number Recruitment Offers from Known Associates by Education Institution of Partipants

Key Finding 6: Youths who accepted recruitment offers were most likely to endorse pro-criminal attitudes that reflected a lack of awareness about how such activities affected others, impulsivity, and a lack of awareness of the illegality of scam-related activities.

70.9% of those involved in illicit scam-related activities endorsed pro-criminal attitudes that reflected a lack of awareness about how such activities affected others (e.g., "I thought it was harmless to others"; see Figure 23). Another common behavioural attribution among participants of scam-related activities was impulsivity (e.g., "I didn't think too much and just wanted to try it out"; 36.4%). Finally, 30.9% of participants endorsed attitudes reflecting a lack of legal awareness about illicit scam-related activities. Specifically, that they were unaware that such activities were illegal or that legal punishment against such activities would be strictly enforced.

Key Finding 7: Youths who rejected recruitment offers tended to be sensitive to potential punishment, aware of the illegality of illicit scam-related activities, and possess prosocial identities.

The majority (75.3%) of participants who rejected recruitment offers endorsed anti-criminal attitudes that reflected a sensitivity to the risk of punishment and consequences (e.g., "the risk of doing it is not worth it"; see Figure 24). Mirroring those involved in scam-related activities, 73.4% of this group cited the illegality of scam-related activities as a reason for rejecting recruitment offers. Finally, 61.0% of those who rejected recruitment offers endorsed anti-criminal attitudes that reflected a prosocial identity (e.g., "someone like me doesn't do such things"). Interestingly, this contrasts with the group involved in scam-related activities, most of whom distanced themselves from attitudes that reflected an antisocial identity (see Figure 23).

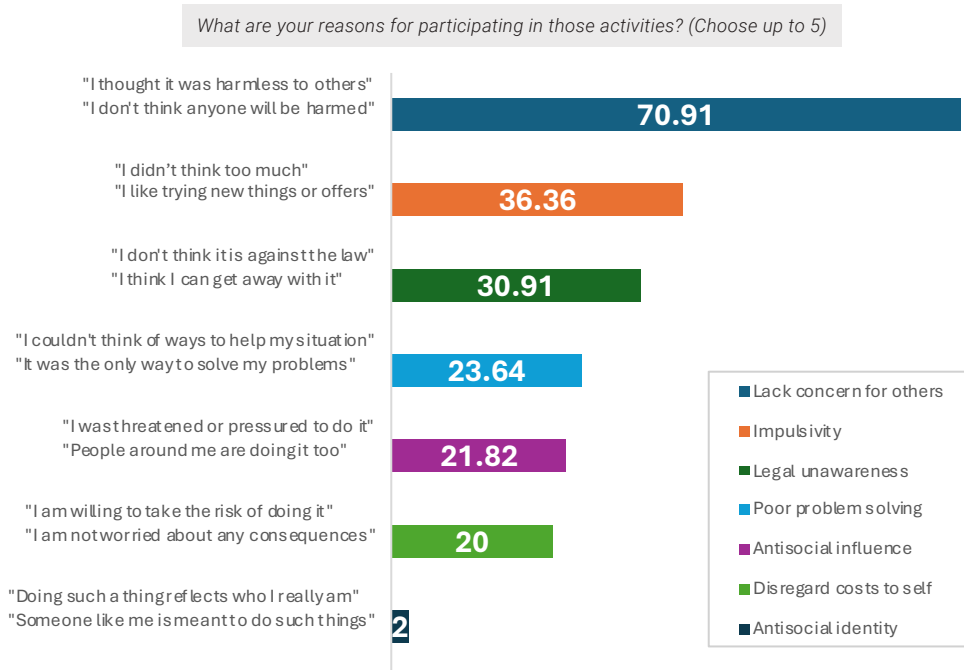


Figure 23. Pro-Criminal Attitudes Endorsed by Participants of Scam-Related Activities

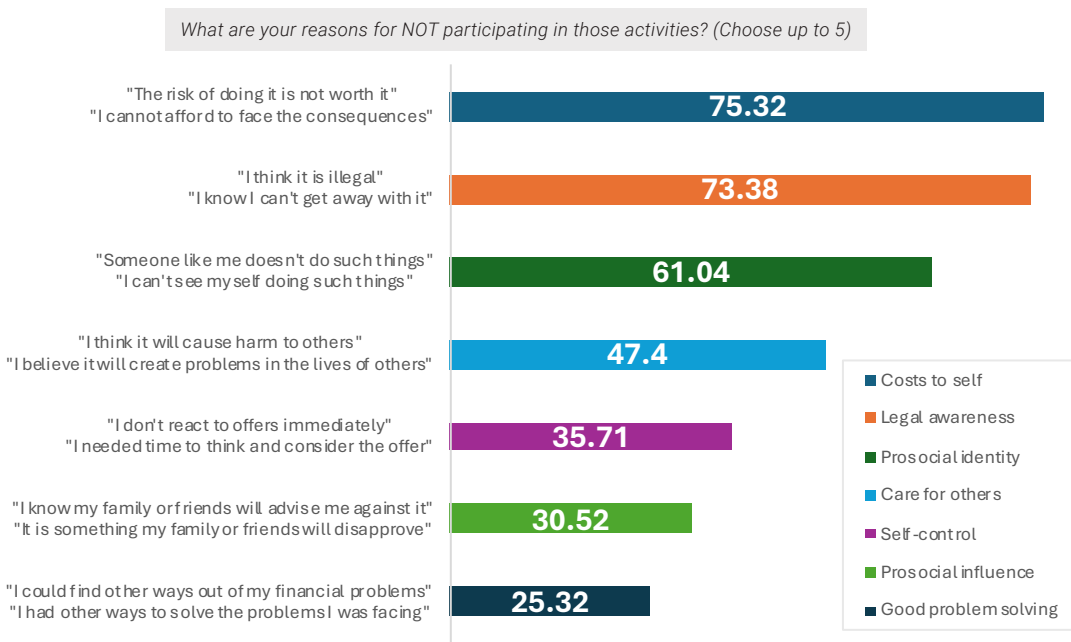


Figure 24. Anti-Criminal Attitudes Endorsed by Participants Who Rejected Recruitment Offers

Key Finding 8: Increased adoption and engagement in anti-scam behaviours were associated with lower exposure to illicit recruitment offers from strangers online.

A large majority (94.0%) of participants limited the sharing of personal information on social media (see Figure 25). Reporting scam-related phone numbers, persons, or accounts was also a frequently adopted anti-scam behaviour among participants (see Figure 26). However, the proportion of participants who downloaded ScamShield app was relatively low (29.0%).

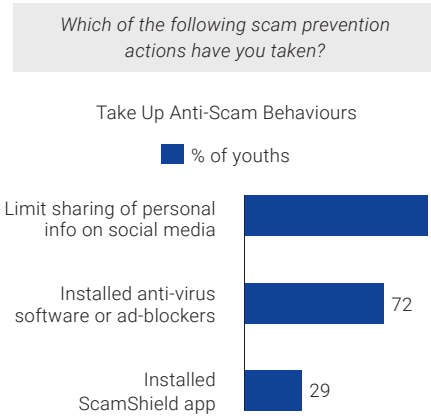


Figure 25. Adoption of Anti-Scam Behaviours

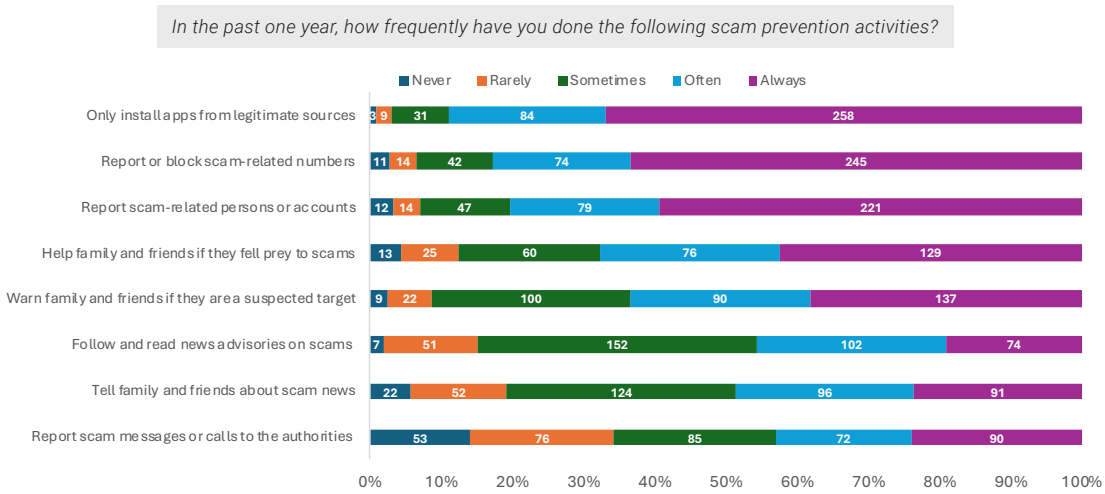


Figure 26. Frequency of Anti-Scam Behaviours

A regression analysis revealed that greater take-up of anti-scam behaviours predicted significantly lower exposure to recruitment offers originating from strangers online (i.e., being approached by a stranger on an online messaging platform; see Figure 27), R^2 = 0.01, $F(1, 388) = 4.2$, $p = 0.04$. Greater frequency of engaging in anti-scam behaviours was also significantly associated with a lower exposure to recruitment offers from strangers online (see Figure 28), $R^2 = 0.01$, $F(1, 388) = 5.00$, $p = 0.03$.

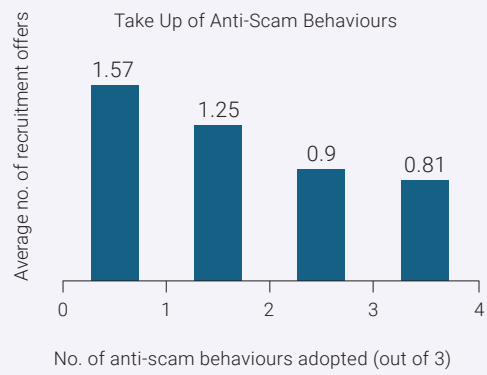


Figure 27. Average Number of Online Recruitment Offers Received by Adoption of Anti-Scam Behaviours

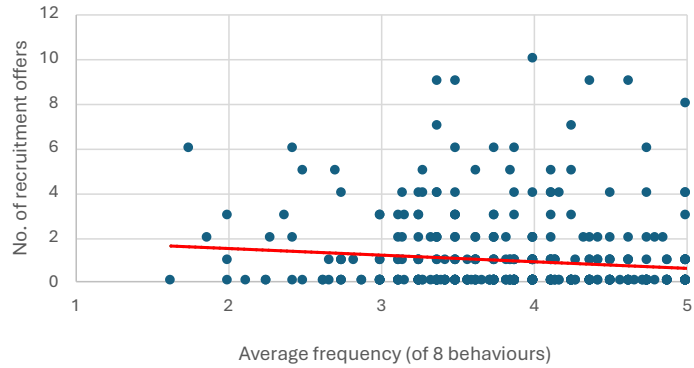


Figure 28. Number of Online Recruitment Offers Received by Frequency of Anti-Scam Behaviours

Figure 29. Summary of Key Findings

Receiving Recruitment Offers for Illicit Scam-Related Activities

- One in two youths received recruitment offers to take part in illicit scam-related activities
- Scam victims, males, and younger youths were more likely to receive recruitment offers for illicit scam-related activities

Responding to Recruitment Offers for Illicit Scam-Related Activities

- One in four youths who received offers accepted them
- Polytechnic students were three times more likely to accept recruitment offers compared to Junior College and University students

Sources of Recruitment Offers for Illicit Scam-Related Activities

- While online, anonymous recruitment offers were far more common than those that originated from a known associate, the latter was four times more effective at recruiting youths

Motivations for (Not) Accepting Recruitment Offers

- Youths who accepted recruitment offers were most likely to endorse pro-criminal attitudes that reflected a lack of awareness about how such activities affected others, impulsivity, and a lack of awareness of the illegality of scam-related activities
- Youths who rejected recruitment offers tended to be sensitive to potential punishment, aware of the illegality of illicit scam-related activities, and possess prosocial identities

Anti-Scam Behaviours and Exposure to Recruitment Offers

- Increased adoption and engagement in anti-scam behaviours were associated with lower exposure to illicit recruitment offers from strangers online

DISCUSSION AND IMPLICATIONS FOR PREVENTIVE MEASURES

Youth Exposure and Involvement

The results of the survey show a significant number of youths in this sample were actively recruited and decided to involve themselves in illicit scam-related activities. This was despite the fact that the sample consisted of tertiary level students who participated in a government-affiliated crime-solving competition. Although the sample was not nationally representative, and the findings should be interpreted with caution, these results converge with local crime statistics, which illustrate a growing number of Singaporeans involved in money mule offences, around half of which are under the age of 25 (Tan, 2023). Both data sources suggest that youth involvement in illicit scam-related activities could be a pressing issue that may warrant further attention from both researchers and policymakers.

Should cases of youth involvement in illicit scam-related activities continue to rise despite legislative amendments, policymakers could consider additional upstream measures to combat the issue. For instance, introducing limits on the number of bank accounts youths can open. This may be effective in prohibiting them from engaging in scam-related activities, while introducing minimal inconvenience to youths, who are less likely to require multiple bank accounts for legitimate financial purposes. Such a measure would be akin to regulatory controls on prepaid SIM cards by the Ministry of Home Affairs (MHA) and Infocomm Media Development Authority (IMDA), wherein an individual may only subscribe to up to three prepaid SIM cards across Singapore's various mobile service providers (Infocomm Media Development Authority, 2014).

Scam Victimisation and Exposure to Recruitment Offers

In the current survey, scam victims were more likely to receive recruitment offers, and received more offers on average compared to scam evaders. These results suggest there may be a nexus between scam victimisation and recruitment for illicit scam-related activities. It is not uncommon for scam syndicates to recontact their victims or sell their victim lists on the dark web for the purpose of re-victimising individuals who have shown to be vulnerable to scams (Commodity Futures Trading Commission, n.d.).

Providing further evidence of the link between scam victimisation and exposure to recruitment offers, the survey also found that increased adoption and engagement in anti-scam behaviours predicted less illicit recruitment offers from strangers online. This indicates that anti-scam behaviours may provide some guard against such online recruitment offers. For instance, the download of the ScamShield app filters possible scam text messages (ScamShield, n.d.). If scam syndicates recruiting youths for illicit activities use similar contact methods, their efforts can be curtailed through the adoption of ScamShield.

Taken together, both findings indicate that scam syndicates may be leveraging a similar set of contacts or contact methods to simultaneously reach potential scam victims and recruit for illicit scam-related activities. Furthermore, that individual measures to guard against scam victimisation may also have the added utility of protecting against exposure to recruitment offers for scam-related activities. This reaffirms comprehensive government efforts to educate the public on scam victimisation through the "I Can ACT Against Scams" campaign. By adding security features such as ScamShield, citizens could be provided with additional protection against both from scam attempts and illicit recruitment offers.

Gender and Participation

While men received more recruitment offers on average than women in this survey, there were no significant differences in the proportion of men and women who participated in illicit scam-related activities. This null relationship runs contrary to the wealth of literature that suggests that men are significantly more likely to be involved in criminal activities (Rebellon et al., 2016). Between 2018 and 2022, there were three to four times more male youth offenders compared to those who were female across all crime types in Singapore (National Committee on Prevention, Rehabilitation, and Recidivism, 2023). Perhaps, this unexpected finding can be reconciled by other research that

suggests that male youths tend to have more antisocial peers than female youths, which results in greater rates of delinquency (Jennings et al., 2010). In the context of illicit scam-related activities, the prevalence of anonymous, online recruitment may indiscriminately target both male and female youths, thus levelling the traditional gender gap in offending (Arevalo, 2015). Overall, this null finding indicates that prevention efforts against youth involvement in illicit scam-related activities should not target only men, but women as well.

A Link Between Educational Institution and Participation?

Although the survey showed that Polytechnic students were three times more likely to accept recruitment offers compared to Junior College and University Students, likely because they received significantly higher number of recruitment offers originating from social contacts, the possible explanations are unclear. Since the sample was not nationally representative and did not include all major youth institutions (i.e., secondary schools, Institutes of Technical Education), the findings presented should be interpreted with utmost caution. Instead, since the current survey has pointed to possible links between educational institutions and scam-related activities, future research should explore this relationship and mechanisms undergirding these links. Subsequently, such research could inform targeted policies and public education efforts.

The Role of Antisocial Influence

The survey found that online, anonymous recruitment offers were about three times more common than those that originated from a known associate. These results converge with research and media reports of online advertisements for illicit scam-related activities, broadcasted on platforms such as Telegram and Instagram (Fintrail, 2022; Hamzah, 2023; Lianhe Zaobao, 2023). Akin to scam victimisation operations, syndicates may focus on quick and anonymous online channels to reach a greater number of potential participants of scam-related activities, while reducing the chance of detection (Vedamanikam & Chethiyar, 2020).

More interestingly, despite there being far more offers from online, anonymous sources, those that originated from a known associate were about four times more successful at recruiting participants for illicit scam-related activities. This finding aligns with existing research that indicates that social network recruitment for illicit scam-related activities is highly effective. According to Bekkers et al. (2023), individuals tend to feel pressured to accede to requests from family members or friends, even when they are illicit in nature (Bekkers et al., 2023).

Furthermore, to avoid social rejection among their peer groups, youths may accept their peers' recruitment offers for illicit scam-related activities (Arevalo, 2015). Even when youths are able to resist such peer pressure, antisocial peers may continue to flaunt ill-gotten gains from their own participation in scam-related activities, culminating in further and subtle social pressure to get involved in similar illicit activities (Orjiakor et al., 2022). Taken together, existing literature and the current survey finding highlights the power of antisocial influence in the recruitment for illicit scam-related activities.

In light of this finding, another legislative lever policymakers could consider would be to introduce laws criminalising the abetment of young persons to participate in scam-related activities. Locally, there are similar provisions for other types of crimes, such as drug consumption. Under Section 11B of the Misuse of Drugs Act (1973), individuals may face up to ten years' imprisonment for permitting a minor to consume drugs in their possession. Hence, extending similar provisions to scam-related activities may have some deterrent effects on members of scam syndicates who are considering inviting their young family members or peers to join them in participating in these illicit activities.

In addition to legislative levers, public education efforts can also be used to dampen the effects of antisocial influence in the recruitment for scam-related activities. Raising awareness among youths on how these innocuous recruitment offers from friends or family members may look like, and how to say "no", may help youths discern and reject such recruitment offers. Going back to existing drug harms prevention efforts, an example

Figure 30. Poster for Drug Educational Skit

of a similar public education initiative for young people would be an anti-drug educational skit by the Central Narcotics Bureau (n.d.). Through a humorous and light-hearted skit, students are taught about the harmful effects of drug abuse (see Figure 30). The skit also role models how to turn down antisocial peers who may invite them to consume drugs.

Addressing Pro-Criminal Attitudes towards Scam-Related Activities

In the survey, while a majority of those who rejected recruitment offers endorsed attitudes that reflected a prosocial identity, those who accepted them tended to distance themselves from attitudes that reflected an antisocial identity. This latter group is particularly interesting as they seem to hold prosocial identities despite their participation in scam-related activities, which could be argued as an antisocial behaviour. Perhaps, this finding can be reconciled through cognitive dissonance theory, which proposes that individuals experience psychological discomfort when they engage in behaviours that are inconsistent with their identity or beliefs (Festinger, 1957). One way that individuals resolve this discomfort would be to cognitively distort and minimise the significance of the behaviour, such as by convincing themselves the behaviour is one-off or acceptable. Hence, even if involvement in scam-related activities threatened participants' prosocial identities, they may have engaged in similar methods to rationalise or minimise their behaviours to preserve it. Taken together, both findings suggests that across both groups, youths in the sample seem to subscribe to a prosocial identity, which could be protective against further antisocial behaviour (Boduszek & Hyland, 2011).

Existing efforts such as legislative amendments and their accompanying public education initiatives may address the lack of awareness about scam-related activities and highlight the potential criminal punishment that may result from involvement in such activities (Singapore Police Force, n.d.; see Figure 6). However, they may not address other potentially significant pro-criminal attitudes, such as a lack of awareness or concern for how scam-related activities may negatively impact others. Furthermore, the prosocial identity of youths can be further harnessed as a protective factor against scam-related activities.

To address these gaps, public communicators can consider expanding public education campaigns on illicit scam-related activities from merely logic-focused messaging to include emotion-focused messaging. For instance, by raising awareness on how scam-related activities play a role in scam victimisation and their associated monetary losses, youths can be educated on how these activities negatively impact others. Such emotion-focused messaging can also appeal to youths with a strong prosocial identity, as these messages may evoke a sense of empathy and compassion for scam victims. A knife crime campaign by the Ben Kinsella Trust (n.d.) is an example of how emotion-focused crime prevention messaging could look like (see Figure 31). The campaign highlights the lasting mental anguish that bereaved families suffer as a result of knife crime.

Figure 31. Knife Crime Campaign Poster

Additionally, given the legislative amendments and expected uptick of arrests for scam-related activities, there may also be a need for downstream rehabilitative services to prevent the recidivism of scam-related offences. The criminal thinking for scam-related activities may differ markedly from sexual or drug offences, which the Singapore Prison Service (n.d.) currently has specialised programmes for. Hence, further research into the cognitive patterns undergirding scam-related offences may be helpful in the tailoring of such rehabilitative interventions (Orjiakor, 2022).

CONCLUSION

The current survey has established that the issue of illicit scam-related activities may be a concern, specifically among local youths. Additionally, it illustrated the powerful role of antisocial influence in the recruitment for illicit scam-related activities. Finally, the survey highlighted key pro-criminal attitudes associated with involvement in illicit scam-related activities.

However, given the exploratory nature and methodological limitations of the current study, further research is needed for convergent evidence of the findings presented. Nevertheless, this article puts forward five recommendations policymakers and public communicators can consider to combat the issue of illicit scam-related activities, should cases continue to rise despite legislative amendments:

Policy

1. Consumer limits on the number of permissible bank accounts for youths
2. Punishment for abetting youths to participate in illicit scam-related activities
3. Specialised rehabilitation programmes for scam-related offences

Public Education

4. Educate youths on how to identify and reject recruitment offers
5. Emotion-focussed messages for public education campaigns

While the prevention of youth involvement in illicit scam-related activities may be an uphill battle due to the lure of quick and easy cash, such activities are critical to the operations of scam syndicates. Hence, much-needed efforts to tackle illicit scam-related activities play a strategic role in the wider battle against the scams scourge.

ABOUT THE AUTHORS

Clarissa Foo
is a Psychologist with the Home Team Psychology Division of the Ministry of Home Affairs. She holds a Bachelor of Social Sciences (Hons) in Psychology from the National University of Singapore. Her research interests lie in scams, sexual crimes and youth psychology.

Kwek Boon Siang
is a Principal Psychologist who has been with the Ministry of Home Affairs for more than 15 years. He currently holds the appointment of Deputy Director of the Crime and Forensic Psychology Branch at the Home Team Behavioural Psychology Division. His research interests are in violent and sexual crimes, offender risk assessment and rehabilitation, scams, and frontline officers' stress and resilience.

Stephanie Chan
is a Lead Psychologist with the Home Team Psychology Division of the Ministry of Home Affairs. Stephanie's current research interest is in crime and forensic psychology, with recent research focussing on knife crime, youth participation in scams, and the psychology of deception and persuasion, as these have operational applications for cybercrime purposes. Stephanie is a member of the British Psychological Society, and she holds a Master of Science in Forensic Psychology from the University of Leicester in the United Kingdom.

Chen Yongjie
was a Behavioural Sciences Research Analyst under the Crime and Forensic Psychology Branch at the Home Team Behavioural Psychology Division. He is currently a Senior Research Officer at the Corrupt Practices Investigation Bureau utilising psychological methods to support investigation operations, corruption prevention, and organisational development.

Wong Jia Wen
was a research intern at the Home Team Psychological Division of the Ministry of Home Affairs. She is currently pursuing a Bachelor of Social Sciences (Hons) in Psychology at the Nanyang Technological University. Her research interests include social, investigative, and forensic psychology.

REFERENCES

Arevalo, B. (2015). *Facilitators of Financial Crime: An Explorative Research on Money Mules in the Netherlands [Master's Thesis, Utrecht University].*

Aqil, H. M. (2022, September 5). *21-year-old scam victim who became money mule says loansharks still harass her.* Channel News Asia. Retrieved from https://www.channelnewsasia.com/singapore/scam-money-mule-loanshark-laundering-police-2918461

Barclays. (2019, September 19). *Barclays issues warning to university students, as number of under-21s recruited as money mules nearly doubles.* Retrieved from https://home.barclays/news/press-releases/2019/10/barclays-issues-warning-to-university-students--as-number-of-und/

Bekkers, L. M. J., & Leukfeldt, E. R. (2023). Recruiting money mules on instagram: a qualitative examination of the online involvement mechanisms of cybercrime. *Deviant Behavior, 44*(4), 603–619. https://doi.org/10.1080/01639625.2022.2073298

Bekkers, L. M., Moneva, A., & Leukfeldt, E. R. (2022). Understanding cybercrime involvement: a quasi-experiment on engagement with money mule recruitment ads on Instagram. *Journal of Experimental Criminology,* 1-20.

Bekkers, L., Van Houten, Y., Spithoven, R., & Leukfeldt, E. R. (2023). Money Mules and Cybercrime Involvement Mechanisms: Exploring the Experiences and Perceptions of Young People in the Netherlands. *Deviant Behavior*, 1-18.

Ben Kisella Trust. (n.d.). *Knife Crime Posters*. Retrieved from https://benkinsella.org.uk/anti-knife-crime-posters/

Boduszek, D., & Hyland, P. (2011). The Theoretical Model of Criminal Social Identity: Psycho-social Perspective. *International Journal of Criminology and Sociological Theory, 4*(1), 604-615.

Broom, D. (2023, August 8). *How the cost of living crisis affects young people around the world.* World Economic Forum. Retrieved from https://www.weforum.org/agenda/2023/08/cost-of-living-crisis-affects-young-people/

Casey, S., Day, A., Vess, J., & Ward, T. (2013). *Foundations of Offender Rehabilitation. Routledge.*

Central Narcotics Bureau. (n.d.). *Skit for Primary Schools*. Retrieved from https://www.cnb.gov.sg/educational-resources/core-programmes/skit-for-primary-schools

Channel News Asia. (2023, April 23). *Duped into taking a 'business development' job, he was ill-treated, forced to scam by a syndicate*. Retrieved from https://www.channelnewsasia.com/cna-insider/duped-business-development-job-scam-syndicate-malaysian-victim-cambodia-3434171

Cifas (2021, September 15). *Data Exclusively Revealed on BBC's Crimewatch Live Shows 78% Year-on-year Increase in Under 21s Taking Part in Money Mule Activity*. Retrieved from https://www.cifas.org.uk/newsroom/mules-six-months-2021

Commodity Futures Trading Commission. (n.d.). *6 Steps to Take after Discovering Fraud*. Retrieved from https://www.cftc.gov/LearnAndProtect/AdvisoriesAndArticles/6Steps.html

Deloitte. (2024). *2024 Gen Z and Millennial Survey*. Retrieved from https://www.deloitte.com/global/en/issues/work/content/genzmillennialsurvey.html

Dunham, K. (2006). Money Mules: An Investigative View. *Information Systems Security*, 1, 6-10. https://doi.org/10.1201/1086.1065898X/45926.15.1.20060301/92679.2

Fintrail (2020, March 31). *How Social Media is used to Further Financial Crime - Part 1*. Retrieved from https://fintrail.com/news/2020/3/30/how-social-media-is-used-to-further-financial-crime-part-1

Festinger, L. (1957). *A theory of cognitive dissonance*. Row, Peterson and Company.

Hamzah, A. (2023, December 28). *Money mule hiring spree goes digital as crime syndicates turn to Telegram*. The Straits Times. Retrieved from https://www.straitstimes.com/singapore/money-mule-hiring-spree-goes-digital-as-crime-syndicates-turn-to-telegram-platform

Home Team Behavioural Sciences Centre. (2020). *Scammer, Beware: Building Societal Resilience to Scams.* Retrieved from https://www.scamalert.sg/docs/default-source/default-document-library/building-societal-resilience-to-scams-ebook.pdf?sfvrsn=c5328718_2

Hu, Y. T., Liu, Q. Q., Ma, Z. F. (2023). Does Upward Social Comparison on SNS Inspire Adolescent Materialism? Focusing on the Role of Self-Esteem and Mindfulness. *The Journal of Psychology, 157*(1), 32-37.

Infocomm Media Development Authority. (2014, 31 March). *Number of Prepaid Cards per Subscriber to be Reduced to Enhance Security*. Retrieved from https://www.imda.gov.sg/resources/press-releases-factsheets-and-speeches/archived/ida/press-releases/2014/number-of-prepaid-cards-per-subscriber-to-be-reduced-to-enhance-security

Jennings, W. G., Maldonado-Molina, M. M., & Komro, K. A. Sex Similarities/Differences in Trajectories of Delinquency among urban Chicago Youth: The Role of Delinquent Peers. *American Journal or Criminal Justice, 35*(1), 56-75.

Kamil, A. (2022, April 5). *Youth form about half of all scam-related offenders arrested in Singapore: Shanmugam*. Today. Retrieved from https://www.todayonline.com/singapore/youth-form-about-half-all-scam-related-offenders-arrested-singapore-shanmugam-1865081

Leukfeldt, R., & Kleemans, E. E. (2019). Cybercrime, money mules and situational crime prevention: Recruitment, motives and involvement mechanisms. *In Criminal networks and law enforcement* (pp. 75-89). Routledge.

Lianhe Zaobao. (2023, 16 November). 抑制骗案从钱骡着手 *[Suppressing Fraud Starts with Money Mules]*. Retrieved from https://www.zaobao.com.sg/forum/editorial/story20231116-1450228

Lim, C. (2024, March 7). *4 men to be charged for money mule activities, selling Singpass, banking details to scammers*. The Straits Times. Retrieved from https://www.straitstimes.com/singapore/courts-crime/4-men-to-be-charged-for-money-mule-activities-selling-singpass-banking-details-to-scammers

Low, Y. (2022, November 3). *TODAY Youth Survey: Cost of living main source of mental health struggles, amid worries over healthcare and everyday expenses*. Today Online. Retrieved from https://www.todayonline.com/singapore/today-youth-survey-cost-living-mental-health-worries-healthcare-expenses-2033126

Ministry of Home Affairs. (2022, April 5). *Written Reply to Parliamentary Question on Number of Youths Caught for Involvement in Scams in the Past Year.* Retrieved from https://www.mha.gov.sg/mediaroom/parliamentary/written-reply-to-pq-on-number-of-youths-caught-for-involvement-in-scams-in-the-past-year/

Ministry of Home Affairs. (2024, March 7). *Law Enforcement and Other Matters Bill*. Retrieved from https://www.mha.gov.sg/mediaroom/press-releases/law-enforcement-and-other-matters-bill

Misuse of Drugs Act (1973) s 11B (Singapore). Retrieved from https://sso.agc.gov.sg/Act/MDA1973?ProvIds=P12-#pr11B-

National Committee on Prevention, Rehabilitation, and Recidivism. (2023). *Factheet on Youth Delinquency 2023*. Retrieved from https://www.msf.gov.sg/docs/default-source/ncpr/factsheet-on-youth-delinquency2fa97cee-baa3-401c-a986-71eb8871bb0b.pdf?sfvrsn=f3f45658_5

National Crime Prevention Council. (2023, November 28). *Check that you are not walking into a Money Mule trap [Video]*. Retrieved from https://www.youtube.com/watch?v=yA72z-zZHNY

Orjiakor, C. T., Ndiwe, C. G., Anwanabasi, P., & Onyekachi, B. N. (2022). How do internet fraudsters think? A qualitative examination of pro-criminal attitudes and cognitions among internet fraudsters in Nigeria. *The Journal of Forensic Psychiatry and Psychology, 33*(3), 428-444.

Pedro, G. (2022, October 6). *One in 10 young people willing to become money mules in return for cash*. Yahoo Finance UK. Retrieved from https://malaysia.news.yahoo.com/young-people-become-money-mules-for-cash-230137276.html

Pickles, R. (2021). 'Money Mules': Exploited Victims or Collaborators in Organised Crime?. *Irish Probation Journal, 18*, 231-243.

Rani, M. I. A., Zolkaflil, S., & Nazri, S. N. F. S. M. (2023). The Trends and Challenges of Money Mule Investigation by Malaysian Enforcement Agency. *International Journal of Business and Technopreneurship, 13*(1), 37-50.

Raza, M. S., Zhan, Q., & Rubab, S. (2020). Role of money mules in money laundering and financial crimes a discussion through case studies. *Journal of Financial Crime, 27*(3), 911–931. https://doi.org/10.1108/JFC-02-2020-0028

Rebellon, C. J., Manasse, E. M., Agnew, R., Van Gundy, K. T., & Cohn, E. S. (2016). The relationship between gender and delinquency: Assessing the mediating role of anticipated guilt. *Journal of Criminal Justice, 44*, 77-88.

ScamShield. (n.d.). *How it works*. Retrieved from https://www.scamshield.org.sg/android-app/

Shane, H. (2023, June 12). Older people hired as 'money mules' by gangs as cost of living crisis bites. *The Guardian*. Retrieved from https://www.theguardian.com/money/2023/jun/12/older-people-hired-as-money-mules-by-gangs-as-cost-of-living-crisis-bites

Singapore Police Force. (n.d.). *CDSA and CMA Bill Amendments*. Retrieved from https://www.police.gov.sg/Advisories/Crime/CDSA-and-CMA-Bill-Amendments

Singapore Police Force. (2022, March 20). Another 14 Investigated For Their Suspected Involvement In Ponzi-Like Job Scams Involving E-Commerce Affiliate Business (EAB). News. Retrieved from https://www.police.gov.sg/media-room/news/20220320_anthr_14_invstgtd_fr_thr_suspct_invlvmt_in_pnzilk_job_scms_invlvng_ecmrce_afflite_bsnss_eab

Singapore Prison Service. (n.d.). *Psychology Based Correctional Programmes (PCPs)*. Retrieved from https://www.sps.gov.sg/learn-about-corrections/programmes/psychology-programmes/

Tan, C. (2023, August 13). *'I just did it for the money': Why young people become money mules for scammers.* The Straits Times. Retrieved from https://www.straitstimes.com/singapore/courts-crime/money-mules-counsellors-worry-as-police-study-shows-almost-half-of-those-recruited-are-under-25

Vedamanikam, M., & Chethiyar, S. D. M. (2020). Money mule recruitment among university students in Malaysia: Awareness perspective. *Pupil: International Journal of Teaching, Education and Learning, 4*(1), 19-37.

Zawadzka, A. M., Borchet, J., & Iwanowska, M. (2022). Can Self-Esteem Help Teens Resist Unhealthy Influence of Materialistic Goals Promoted By Role Models? *Frontiers in Psychology, 12*. Retrieved from https://www.frontiersin.org/journals/psychology/articles/10.3389/fpsyg.2021.687388/full

The HTPD Brief
Psychological Insights for the Home Team

YOUTH VAPING:
RISKS, PROTECTIVE FACTORS AND POSSIBLE INTERVENTIONS

Leung Chi Ching, Sherrer See
Home Team Psychology Division, Ministry of Home Affairs, Singapore

ABSTRACT

In recent years, the prevalence of vaping, which is illegal in Singapore, has surged among youths in Singapore, highlighting the need to analyse its physical, psychological, and social implications. Vaping is addictive, brings about various harms and is detrimental to users. Its prevalence may also open the door to associated illegal activities (e.g. illicit drug use and vape trafficking). This article adopts a biopsychosocial lens, which delves into interconnections between the biological, psychological, and social elements to understand how these elements play a role in youth vaping behaviours. By understanding risk and protective factors, it aims to better understand the motivations and susceptibility to vaping as well as assess how these factors could lead to associated offending behaviours among youths. This allows for more effective utilisation of these factors to identify or develop effective interventions. Preventive strategies and interventions both local and global will also be examined. This multifaceted review provides insight into the growing world of vaping among youths.

A GROWING PROBLEM

Vaping and the growing vape market is a rising issue, both globally and in Southeast Asia (Tehrani et al., 2022; Van Der Eijk et al., 2022). In 2023, 7,838 persons were caught for the possession or use of e-vaporisers, a 60% increase from the 4,916 in 2022 (Ministry of Health, 2024). More worryingly, the increase in youth vaping is a cause for concern. In 2022, 800 students were reported to have been referred to the Health Sciences Authority for vaping offences, which was a stark increase from the 50 cases between the period of 2018 to 2019 (Tushara, 2023).

The increase in vape usage could entice more vape traffickers to cross into Singapore to sell and distribute vape products illegally. This is evident from an attempted trafficking of more than 58,000 vape products into Singapore in January 2023, which was stopped by the Immigration & Checkpoints Authority (Sun, 2023).

Vaping could also lead to other associated offences. For example, Grant et al. (2019) shows that among a large sample of university students, vaping is associated with the use of other illicit substances. And drug trafficking syndicates in the region appear to be trying to fill such a need or creating a demand; a recent operation by the Central Narcotics Bureau (CNB) found at least 65 vapes containing cannabis (CNA, 2024). Taken into totality, vaping could hinder the government's efforts in enforcing against harmful drugs. Thus, the expanding vape market along with the increase in youth vaping underscores the need for stronger prevention and enforcement efforts.

What are Vapes?

Electronic Nicotine Delivery Systems (ENDS), more commonly known as e-cigarettes or vapes, are electronic devices designed

to vaporise various chemical contents (Oriakhi, 2020). According to the National Academies of Sciences (2018) and Traboulsi et al. (2020), the contents of vape usually involve six components: nicotine, metals, solvents, flavourings, sweeteners, and other compounds. Figure 1 shows the various constituents of a vape.

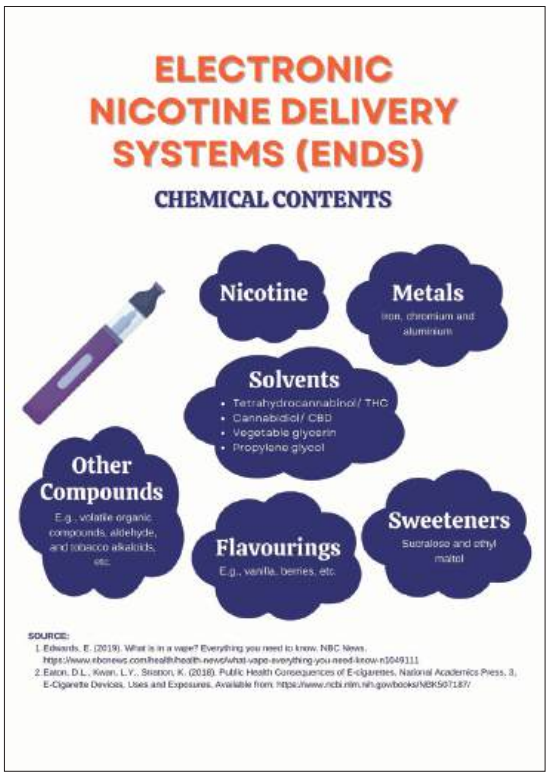


Figure 1. Chemical Contents in Electronic Nicotine Delivery Systems (ENDS)

Legislation

Singapore has taken great efforts to curb vaping through various policies and preventive education. Under the Tobacco (Control of Advertisements and Sale) Act (1993), penalties such as a fine of $2,000 are given to individuals caught purchasing, using or owning vapes. The law also states that individuals are prohibited from importing vapes into Singapore, as well as distributing, selling or possession for sale, where individuals convicted for these activities are liable to a $10,000 fine or imprisonment of six months. Apart from regulation, the Health Promotion Board (HPB) also arranges various preventive education programmes such as assembly skits targeting students on issues of smoking and vaping (HPB, 2024). Cessation programs such as the "I Quit Programme" that started in 2013 also target youths by providing support to encourage them to quit smoking or vaping over a one-month period. However, despite these active steps taken, the number of vape users arrested is still on the rise.

Vaping as a Treatment Tool?

Over the years, there have been debates on vapes' potential for use in smoking cessation. Hartmann-Boyce et al. (2022) found that individuals were more likely to stop smoking for at least six months when using nicotine vapes compared to nicotine replacement therapy. Similarly, Burrowes et al. (2022) found that the "Vape to Quit" strategy achieved successful self-reported smoking cessation rates in half the participants. Although vaping as a treatment tool for smoking could be useful if it works, its actual viability is still doubtful. This is due to insufficient evidence to support the efficacy of vapes for smoking cessation (Banks et al., 2020). Furthermore, vaping has been found to be associated with illicit drug use among students (Grant et al., 2019), which could be a potential consequence of using vapes for smoking cessation. Overall, it appears that the cons of adopting vaping as a smoking cessation tool might outweigh the pros and be not as effective in the long run.

NEGATIVE HARMS OF VAPING

Although few studies have been conducted on the prevalence of youth vaping in Singapore, data from a recent study by Ng et al. (2024) found that among a sample of 550 adults aged 21 to 40 obtained through convenient sampling, 16.9% of respondents reported ever vaping. Data from other countries paint a similar picture. Findings from a Malaysian national survey showed that in a sample of 33,532 students, the prevalence of vaping was 14.9% (Yusoff et al., 2023) while another study by Patanavanich et al. (2021) on youth vaping in Thailand found that the lifetime prevalence of vaping was 7.2%, while the current vape usage was 3.7% among a sample of 6,045 student respondents. Considering the geographical proximity of Malaysia and Thailand to Singapore, these findings highlight the increasing trend and seriousness of youth vaping. While the long-term harms of vaping are largely unknown (Marques et al., 2021) due to it being a relatively new topic of research, the short-term consequences are profound as vaping is associated with various

physical, psychological, and social impacts on youths (Figure 2).

Physical Impacts

Vaping brings about a myriad of physical harms, especially to one's airways and the lung parenchyma (i.e. the portion of the lung involved in gas exchange) (Jonas, 2022). Vaping increases airway resistance and decreases airway conductance (Honeycutt et al., 2022). Thus, youth vapers are more prone to developing respiratory issues like asthma, bronchitis, and respiratory tract irritation (Lyzwinski et al., 2022). In 2019, the EVALI (e-cigarette product use-associated lung injury) outbreak spotlighted the harmful effects of vapes. EVALI is a pulmonary illness associated with vape usage due to a component called 'vitamin E acetate' from tetrahydrocannabinol (THC) vapes (Rebuli et al., 2023). The EVALI outbreak led to numerous hospitalisations in the US (Krishnasamy et al., 2020), especially among the young (18 to 34 years), with the youngest death reported to be a 15-year-old (Van Der Eijk, 2022).

Figure 2. Infographic on the Physical and Psychological Harms of Vaping

Apart from EVALI, vaping devices potentially expose users to heavy metals from the batteries and heating coils that may be carcinogenic, or hazardous to the heart and lungs (Becker & Rice, 2022). The chemicals in vapes could also cause poisoning, burns, and immediate toxicity through inhalation, including seizures (Banks et al., 2023). Other side effects include throat irritation and nausea. Banks et al. (2023) also found that vaping increases heart rate, blood pressure and arterial stiffness acutely after use.

Vaping also brings about structural damages to the brain such as the hippocampus, and limbic system which affects one's emotional regulation (Anand & Dhikav, 2012). Zelikoff et al (2018) found that vaping alters one's central nervous system causing damage to the hippocampus while Codd et al. (2020) found that vaping could potentially cause neurodegenerative disorders such as stroke. Research from Heldt et al. (2020) also found that vaping increases the risk of inflammation thereby affecting one's neurovascular health. Moreover, a review by Wawryk-Gawda et al. (2020) found that vape usage could affect the thalamus influencing sleep (Grossman & Inglese, 2016) as well as the frontal cortex, influencing movement, social cognition and overall behaviour (Kolb & Whishaw, 2003), indicating the structural damage of vaping on the user's brains.

Psychological Impacts

Cognitive Harms

Apart from harms to the body, cognitive and attentional harms could also occur from nicotine vape exposure (Trivers et al., 2021). Nicotine is an addictive substance influencing brain areas involved in emotional and cognitive processing, which is detrimental as brain development during adolescence is extremely sensitive to nicotine's effects (Goriounova & Mansvelder, 2012). In a review by Goriounova & Mansvelder (2012) on youth smokers, they found that youths' working memory and attention are greatly impaired by smoking (as cited in Jacobsen et al., 2005). Although this finding was on smoking combustible cigarettes, it could also apply to vaping due to the similar nicotine mechanisms. Moreover, Xie et al. (2020) reported that adolescent vapers show greater cognitive

impairments such as difficulty concentrating, remembering and making decisions.

Several studies have also reported on psychological impacts on youths after nicotine exposure from vaping. A systematic review by Becker et al. (2021) found that vape usage among adolescents is linked to internalising disorders such as depression, suicidality and disordered eating, and externalising disorders such as attention deficit hyperactivity disorder (ADHD), conduct disorder, impulsivity and perceived stress.

Vaping also increases one's chances of experiencing anxiety symptoms like worries, flashbacks, panic attacks and situational anxieties. A survey conducted by the American Heart Association among teens and young adults (13 to 24 years old) found that nearly 70% of THC vapers (which contain cannabis) and 60% of nicotine-only and dual vapers reported anxiety symptoms in the previous week, in comparison to 40% of non-users, and that more than half of people under all vaping categories reported suicidal ideation within the last 12 months, in comparison to only one-third of non-users (American Heart Association, 2023). This is further supported by Javed et al. (2022) who also found that vape use is associated with depression, suicidal ideation, and suicide attempts.

However, it should be noted that vape usage and depression could also be bi-directional, where having depression influences youths to use vaping as a means to reduce these negative thoughts (Lechner et al., 2017). Behavioural changes such as increased hyperactivity and impulsivity have also been found to be associated with vaping because of nicotine exposure to the brain (Jones & Salzman, 2020).

Without early intervention, youth vapers could deviate to other risky behaviours such as substance abuse. Research by the Columbia University Mailman School of Public Health on 50,000 US adolescents found that vaping is not an isolated behaviour but is tied to substance abuse (Kreski et al., 2023). The experimentation with vape equipment is cited by Giroud et al (2015) to be an effective transitional tool – from vaping nicotine to vaping other drugs like cannabis. The nicotine in vape stimulates receptors in the brain, triggering a rewarding effect, known as psychostimulant reinforcement and reward (Ren & Lotfipour, 2019). The effects of nicotine and other drugs are further enhanced by repeated exposure: the more teenagers expose themselves to nicotine, the greater their sense of satisfaction. This effect then increases the likelihood that young people develop a reliance on such substances (O'Dell, 2009). Studies have shown that adolescents who smoke cigarettes or use vapes are far more prone to binge drinking than non-smokers (Kristjansson et al., 2015). Further studies have also found similar patterns between nicotine use and the use of other drugs such as cannabis (Unger et al., 2016).

Social Impacts

Vaping could also bring about societal impacts on families, school performance and increase in crime rates. Interviews conducted with parents of youth vapers by Davey (2022) unveiled the familial impacts of youth vaping on family relationships, where youths addicted to vaping get physically or verbally violent towards their parents. Davey also discussed the adverse impact of vaping addiction on youth's academic lives, further substantiated by Augenstein et al. (2024) who found that vape usage among adolescents is associated with poor academic performance. Vape usage could also lead to increase in antisocial behaviour where vaping among youths is associated with delinquency (Jackson et al.,2019). Furthermore, with the demand of vapes increasing in Singapore, this could increase the rates of vape smuggling into Singapore.

Impacts on the physical, psychological, and social domains highlight the consequences of vaping. Thus, interventions must be implemented to curb vaping among youths. Before developing interventions, risk and protective factors must be understood to map these factors onto specific interventions for effective development of solutions.

RISK FACTORS

To better conceptualise our understanding of risk factors, the biopsychosocial model (Figure 3) is proposed as a framework (Engel, 1977). The biopsychosocial model postulates the importance of examining individual biological, psychological and social factors as well as the interactions between them to provide a holistic understanding of the issue to address the needs of individuals (Borrell-Carrio, 2004).

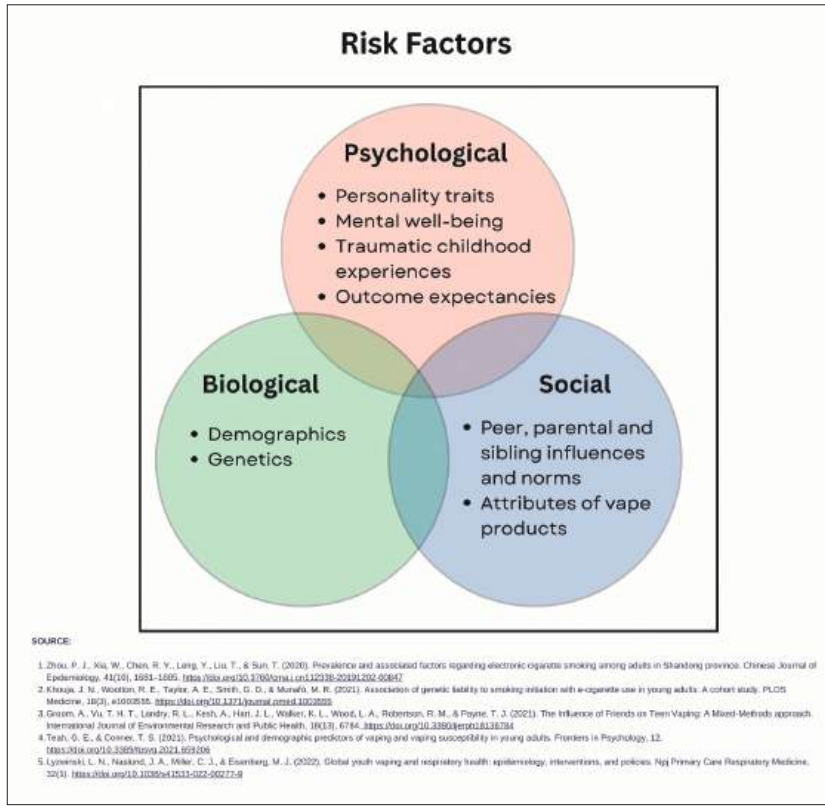


Figure 3. Biopsychosocial Framework (Risk Factors)

Biological Factors

The biological perspective investigates various biological factors that could contribute to youths' susceptibility to vaping, such as demographics (e.g. age and gender) and genetics.

Demographics. Youths are highly susceptible to vape usage due to their age. In Singapore, a large demographic of individuals who use vapes are of a younger age (20 to 28 years old) as seen in the trend of vaping among students over the past 3 years (CNA, 2023). This is further corroborated by Zhou et al. (2020) who has found higher susceptibility to vaping among those from 15 to 30 years old. Being male is also associated with higher susceptibility to vaping (Ahmed et al., 2021). A study among US vape users also support these findings – males below 35 years old are more susceptible to vaping (Mayer et al., 2020; Coleman et al., 2014).

Psychological Factors

The psychological perspective investigates psychological factors that could contribute to one's susceptibility to vaping such as personality traits, impulsivity, self-control, sensation-seeking, and anxiety sensitivity.

Personality Traits. A study by Munafo et al. (2007) found that being high in extraversion and neuroticism increases susceptibility to smoking, while a study by Teah & Conner (2021) found higher openness to be associated with vaping due to the increased willingness to be open to various experiences, such as vaping. Next, findings by Mai et al. (2022) found that low agreeableness is associated with the use of vapes. They attributed this finding to the fact that individuals with high agreeableness adopt more problem-focused coping styles which is the converse of individuals

with low agreeableness. Finally, Teah and Conner (2021) found that being low on conscientiousness predicts vaping. Apart from the Big 5 Personality traits (namely Conscientiousness, Agreeability, Neuroticism, Openness to Experience and Extraversion), impulsivity is also found to be associated with vaping among youths. Mittal et al. (2022) investigated the facets of the impulsivity trait and found that two facets – higher sensation seeking, and lack of premeditation – associate with higher vape usage.

Mental Well-being. Mental health factors such as anxiety, stress, depression, and substance abuse could lead to youth's susceptibility to vaping (Conway et al., 2018; Lee et al., 2019). Most prominently, depression and anxiety have the highest association with vaping prevalence. Scully et al. (2023) found a strong association between symptoms of depression and susceptibility to vaping. Lechner et al. (2017) also found a bi-directional relationship between vaping and depression where individuals with depression are more likely to engage in vaping and individuals who vape are more likely to have depression. Anxiety is also a prominent mental health factor that could contribute to susceptibility to vaping. Teah & Conner (2021) found that anxiety strongly predicts youths ever using vapes. Stress has also been found to be highly associated with vaping behaviours among youths. A study by Donaldson et al. (2022) found that youths use vapes for stress relief. These studies highlight that stressors faced by youths increase the susceptibility to vaping. This is due to youths wanting to alleviate negative affect and thus turn to vapes as a means of coping and self-medication. The usage of vapes for stress management may create a reinforcing cycle of vaping among youths.

Outcome Expectancies. This refers to anticipated positive or negative consequences due to an enacted behaviour (Reesor et al., 2017). Youths have insufficient negative perceptions of the safety of vapes, therefore increasing their positive outcome expectancies, making youths susceptible to vaping (Hamberger et al., 2022). Pokhrel et al. (2019) found that having higher positive outcome expectancies (e.g. social enhancement, affect regulation and positive sensory experience) is associated with increased vape usage which is supported by other studies (Barker et al., 2019; Latimer, 2023).

Closely related to anxiety and outcome expectancies is anxiety sensitivity (AS) where "one's fear of internal bodily sensations associated with anxiety due to the concern that it is potentially dangerous" (Reiss, 1987) is also associated with vaping. Garey et al. (2019) found a significant association between AS and youth's perception of the risks, benefits, and positive outcome expectancies of vapes. The study also found that vapers high in AS are highly sensitive towards their bodily responses upon the usage of vapes, which either reinforces future use or encourages the lack of use. A study by Manning et al. (2021) investigated the effects of AS on vape dependency among youths and found AS to be strongly associated with the perceived barriers to quitting vapes and contributing to cravings for them.

Traumatic or Adverse Childhood Experiences. Youths' traumatic or adverse childhood experiences increase their susceptibility to vaping (Shin, 2021) where childhood emotional abuse and neglect is found to be associated with lifetime vape usage (Shin et al., 2019). This is further corroborated by Williams et al. (2020) who found a strong association between adverse childhood experiences and early initiation of vape products. The accumulation of multiple stressors could exacerbate the relationship between these stressors and vape usage (Erhabor et al., 2023).

Other Psychological Constructs. Self-control and curiosity are other psychological constructs that could increase youth's susceptibility to vaping. Self-control – the ability to delay immediate gratification for a later reward (Ainslie, 1975) – is an important construct in evaluating susceptibility to vaping. Low self-control among youths is found to increase susceptibility to vaping. Sutherland et al. (2022) found that youths low in self-control and high in depression report higher intentions of vape usage. This finding highlights the importance of self-control in buffering against mental health risk factors (i.e., depression) leading to vape usage.

Finally, youths might also be susceptible to vaping due to curiosity. The 2014 National Youth Tobacco Survey conducted among middle and high school students in the United States found that curiosity is a major risk factor for vape usage among adolescents (Margolis et al., 2016). High school students tend to be extremely curious

about vaping which is enhanced when youths have lower perceptions of being harmed by the vapes. A study by Pettigrew et al. (2023) found 56% of youths to be curious about vapes, increasing their susceptibility to them. This curiosity might also arise from the marketing of these vapes (i.e. flavourings) increasing their appeal (Pepper et al., 2016). This emphasises the interaction between the psychological and social domains in influencing susceptibility to vaping. This curiosity is also a similar precursor for other risky or early offending risk factors (Mayone & Arneklev, 2015).

Social Factors

The social perspective looks at social, environmental, and cultural factors that could contribute to one's susceptibility to vaping, such as cultural norms, peer, parental, and sibling influences; attributes of vape products, marketing of vape products, and spirituality.

Peer Influences and Youth Culture Norms. Generational culture is a crucial influence on youths' susceptibility to vaping. This involves the normalisation of vaping behaviour among youths. The mechanism behind this culture lies in peer influences. Peer influences (i.e., social norms and conformity) is a common risk factor that increases youths' susceptibility to vaping. Social norms refer to behaviours, feelings and thoughts seen as normal within a group (Reese et al., 2019). Vaping is popular among youths where even those who do not vape are aware of its existence and popularity (Park et al., 2019). Vaping is normalised as a social practice linked with global youth culture (Scheffels et al., 2023).

Various studies have found that peers strongly reinforce vaping among youths (Groom et al., 2021; Ling et al., 2023; Becker & Rice, 2022). Exposure to these vaping norms might lead to conformity among youths which is not optimal as adolescents are found to conform more compared to adults (Minich et al., 2023). Vaping initiation is more likely to occur if people within youths' social networks also start vaping, the converse is also true where vaping cessation occurs if their social network stops vaping (Christakis & Fowler, 2008; De Vries et al., 1995).

Parental and Sibling Influences. Parents and siblings are also crucial risk factors in youth's susceptibility towards vaping. Parental attitudes, knowledge, and usage of vapes could contribute to youth vaping. According to Fite et al. (2018), parental attitudes are strongly associated with youths vape usage where if parents believe that vaping is bad, their child will adopt similar attitudes and be less susceptible to vaping. In another study by Trucco et al. (2021), they found that when parents lack knowledge on the harmful effects of vapes, they are unable to fully understand these risks and thus unable to develop the attitudes needed to deter youths from vaping. Parental usage of vapes also influences youths' usage due to modelling of behaviour (East et al., 2018).

Sibling influences also play a critical role in influencing youths' expectations and intentions to use substances (Maiya et al., 2023; Slomkowski et al., 2005; Wamba et al., 2023). Whiteman et al. (2016) have posited that older siblings can serve as direct or indirect influences on youths' future intentions to vape. Older siblings serve as direct social influences through modelling behaviours. They also serve as indirect cognitive influences through changing youth's perceptions, e.g. informing their siblings of the benefits of vapes (Maiya et al., 2023).

Attributes of Vape Products and Marketing. Besides the social and cultural factors, vapes have various attributes that increase their marketability for youths. These include the discreetness of vapes, aesthetics, affordability, flavouring and ease of access. Vapes are discreet products and easy to hide (Lyzwinski et al., 2022; Gilmore et al., 2023) – a functionality attractive to youths as it allows them not to get caught easily. This discreetness helps when youths want to vape at home, and the absence of smell when using a vape is a further pull factor (Neo & Tay, 2022). Vapes are also easy to access (Lyzwinski et al., 2022) and extremely fashionable (Zhong et al., 2022). Vapes have also developed aesthetically over time to appeal to youths (Holtermann, 2023) and are affordable (Ling et al., 2023). Youths interviewed in Singapore have cited the cheaper price of vapes compared to combustible cigarettes, while containing more nicotine, making it "worth their money" (CNA, 2023).

The flavourings in vapes could increase youth's liking for it and increase susceptibility towards vaping (Zhong et al., 2022; Lyzwinski et al., 2022; Hamberger et al., 2020). According to Patel et al.

(2016) youths are more susceptible to flavour marketing of vapes than adults. Landry et al. (2019) also found that the flavours of vapes contribute to vaping initiation and greater satisfaction with the experience, reinforcing the cycle of vaping.

To cater to youths, vape products focus on appealing flavours like fruit and candy (Goldenson et al., 2019). These flavours then lead to susceptibility to consumption through their enticing names and diversity which are attractive to youths (Meernik et al., 2019; Shang et al., 2018). Moreover, these flavoured vapes mask the harsh nicotine scents which youths might not find enjoyable (Griffiths et al., 2011). Finally, these flavours assist in reinforcing the nicotine addiction among youths (Donaldson et al., 2017) further keeping them hooked.

In Singapore, apart from flavours, vapes are also marketed through online retailing. Youths are avid users of social media, with users aged 19 to 25 making up the majority of Instagram users based in Singapore (35.52%) (Satistia, 2023), while the largest group of Telegram users worldwide is between the ages of 25 and 34 (>29%) (Statista, 2023).

Vape distribution is largely reliant on the messaging platform Telegram. These Telegram channels are popular and public for anyone to access (Baker & Ang., 2021). In Singapore, the Health Sciences Authority has cautioned 16 social media services and e-commerce platforms for displaying vaping content on their sites (Ministry of Health, 2024). The diverse platforms further facilitate this ease of purchasing due to their wider exposure to youths. Furthermore, the online platform is largely unregulated which serves well the distributors of vapes, given the current legislation.

PROTECTIVE FACTORS

Protective factors are factors that reduce or mitigate risk factors and understanding these factors allows for the effective design of interventions through strengthening these protective factors among youths.

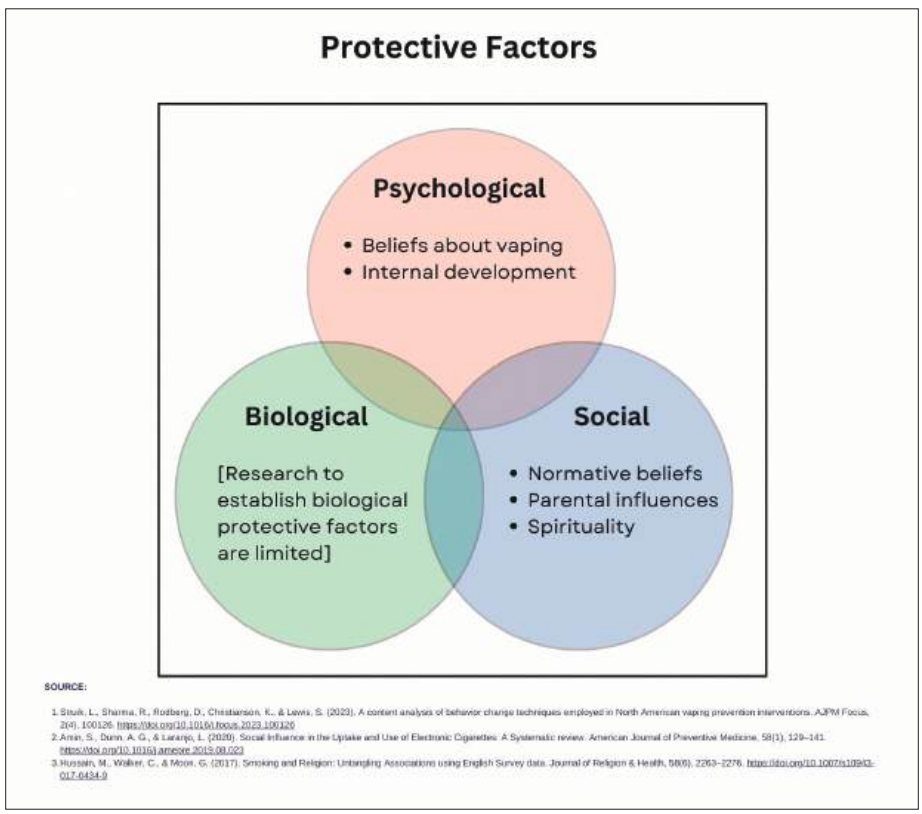


Figure 4. Biopsychosocial Model (Protective Factors)

Psychological Factors

Several psychological protective factors reduce the risk of youth vaping. They include beliefs about vaping, youths' internal development and emotional responses.

Beliefs about Vaping. Youths have various beliefs about vaping which could be an asset in deterring them from vaping. Behavioural beliefs about vaping are found to be a protective factor against vaping. Behavioural beliefs refer to the perceived advantages or disadvantages associated with vaping. Youths who do not vape report negative beliefs towards vaping such as believing that vaping is bad for their lungs (Struik et al., 2023; Rohde et al., 2018). These beliefs about the perceived consequences of vaping are essential in curbing vaping behaviour, where decrease in positive expectations of vapes see a 67% reduction in youth's likelihood of vaping (Moustafa et al., 2021).

Psychological Development and Growth. Youths' psychological development is an asset in deterring vaping. Some of these developments include beliefs about their future orientation, self-efficacy, social competency, and positive identity. Firstly, having a positive future orientation refers to youths having clear goals, good planning, and an ability to overcome challenges (Johnson et al., 2016). A study by Szoko et al (2021) found positive future orientation to be associated with lower prevalence of lifetime vaping; youths with expectations for their future are protected against negative health outcomes.

Self-efficacy, which refers to an indiviudal's belief in his or her own ability to carry out certain behaviours (Bandura, 1977) is also associated with vaping deterrence. Self-efficacy in this case refers to the degree of confidence youths have in abstaining from vaping. High self-efficacy decreases risk-taking behaviours and influences health decisions among youths (Schwarzer & Luszczynska, 2005), contributing to positive mental wellness (Jerusalem & Hessling, 2009), and decreasing the effects of adverse psychological well-being (i.e., depression and anxiety) which has been found by some studies to increase susceptibility to vaping. Various studies have shown that having higher self-efficacy lowers one's susceptibility to vaping (Struik et al., 2023; Barrington-Trimis et al., 2015; Durkin et al., 2020; Jones et al., 2020).

Social Factors

The social perspective looks at the social, environmental, and cultural influences on vaping behaviours among youths.

Normative Beliefs. Normative beliefs refer to individual's beliefs about whether their social circle deems a particular behaviour acceptable. Struik et al. (2023) has found that youths who do not vape report choosing not to vape because of disapproval from their social circle. Youths who do not vape also have the perception that daily vape use is socially unacceptable and that their friends and family disapprove, hence deterring them from vaping (Katz et al., 2019).

Parental Influences. Social influences from one's social networks and societal norms greatly influence youth's vaping behaviour (Amin et al., 2020). Parental influences (i.e., parental education, monitoring, and connectedness between parent and child) have been found to be strong protective factors against youth vaping. A study by Kaleta et al. (2016) and Rhode et al. (2018) found that parents with higher education act as a protective factor against vape usage as they are better aware of the harms of vaping, and are well placed to inculcate this knowledge in their children. Furthermore, parental monitoring, which refers to parental supervision of their children (Dishion & McMahon, 1998), is also an effective protective factor (Lessard et al., 2014). Parental connectedness, which refers to the connections formed with one's family and the feeling of being cared for and loved (Foster et al., 2017), also acts as a protective factor. Wilhelm et al. (2021) found that parental connectedness could deter vape usage among youths. Similarly, Szoko et al. (2021) also found that positive parent-child relations through open communication and high mutual trust could deter health-risk behaviours like vaping.

Spirituality. Spirituality could also influence susceptibility to vaping. A study by Hill et al. (2022) found that conservative Catholics were more likely to reduce vape usage during the pandemic compared to individuals with no religion. Furthermore, Hussain et al. (2017) has found that across youth and adult groups, those with no religion have higher occurrence of smoking. When comparing across religion groups, Muslim youths are found to be less likely to be smokers compared to Christians or those with no religion. Though their findings are on smoking, this association could also be applied to spirituality and vaping, due to similar mechanisms such as individuals being bonded with communities with abstinent norms and expectations about the act of smoking.

Though we have a preliminary understanding of the protective factors that could help with vaping deterrence among youths, more localised findings need to be available to enhance prevention efforts through a strength-based approach which focuses on the strengths of the youth instead of looking primarily at their deficits (McCashen, 2005).

PREVENTION AND CESSATION INTERVENTIONS

With the increasing prevalence of vaping, prevention education and interventions have in recent years been stepped up to curb vaping in Singapore.

Prevention Efforts

In Singapore, the Health Promotion Board (HPB) offers primary prevention efforts to curb vaping among youths. These include a vape-free campaign targeting youths through digital platforms to communicate the harms of vaping. Furthermore, assembly skits are also organised in schools to educate secondary school students on the harms of vaping. However, given that vaping is still prevalent, more must be done to ensure the effectiveness of these initiatives.

Evidence-based programs are programs that are effective due to the findings from the extensive evaluations (Cooney et al. 2007). Evidence-based prevention efforts could be incorporated into current prevention efforts. They aim to educate and increase youth's knowledge about the risks of vaping as well as increase youth's risk beliefs about vapes and teach them practical skills about rejecting vaping. Generally, most of the youth participants who have undergone these programmes appear to accept them, indicating preliminary success. The US Food and Drug Administration's Real Cost Campaign features prevention videos effective in reducing youth's susceptibility to vaping as well as shows increased risk beliefs about vaping (Noar et al., 2022). The CATCH My Breath programme is a preventive US education programme targeting youth's perceived consequences of vaping, identifying risk factors and advertisements (Kelder et al., 2020). It has been shown to reduce susceptibility to vape usage and improved knowledge while decreasing perceived positive outcomes of vaping. Next, the tobacco prevention toolkit is a vaping prevention curriculum from the US which has improved students' perceptions of vapes as well as their knowledge and refusal skills (McCauley et al., 2023). These preventive educational programmes have been effective in improving knowledge on vaping, increasing risk beliefs about vaping, and reducing susceptibility towards vaping.

Prevention efforts involving the community could help prevent youth vaping. Research from Tinner et al. (2024) found that community mobilisation interventions could be effective in reducing youth risk behaviours such as tobacco smoking, which could be applied to vaping due to the presence of nicotine in both products. However, for these community interventions to work, the environment where these risky behaviours occur at must be changed with the assistance of the community.

Table 1. Prevention Efforts – Community

Prevention Efforts	Summary
Parental knowledge and media mediation in preventing adolescent e-cigarette usage (Choi et al., 2022)	Findings from a US study showed that parental knowledge shapes adolescents' views towards vaping where they believe that substances are harmful. Parental media mediation (i.e., actively discussing media limiting exposure to pro-vaping content) was positively related to the perceived harms of vaping. These findings highlight the importance of family-based interventions such as monitoring adolescent media consumption.
Youth's perceived perception of parental knowledge (Mantey et al., 2022).	Findings from a US study showed that youth's perceptions of higher levels of parental knowledge of their location, activities and peer groups were associated with lower risks for vaping. The study's implications involve directly engaging the parents/ guardians and enhancing their parental knowledge.
School regulation for vaping (Nicksic et al., 2018)	In a US study where school administrators perceived vaping to be an issue, the written school policy positively impacted student's vaping prevalence, lowering students' susceptibility to vaping.
Vaping control policies on school property (Milicic et al., 2018)	In a Canadian school, findings showed that bans on vaping in school property could prevent use of vapes and school-level policies were found to be effective.

Future consideration for preventive education in Singapore could allow youths to have a stake in designing interventions, and conduct small-group discussions in schools to discuss facts and myths about vaping.

Cessation Interventions

Apart from prevention efforts, HPB also offers cessation interventions like the 'I Quit Programme' introduced in 2013 where individuals recovering from smoking or vaping are supported for up to 6 months to quit. This treatment programme involves a personalised approach depending on the type of smoker where they receive either an SMS tip or calls from trained coaches as well as counselling. To encourage completion of the programme, individuals are entitled to receive incentives upon reaching milestones.

Another intervention in Singapore organised by the MacPherson Youth Network is the anti-vape pilot campaign 'Drop It, Stop It!" where students who drop their vapes into the bin provided can receive a $30 incentive (Wong, 2023).

Despite the above interventions, some current gaps exist. Existing cessation interventions from other countries involve environmental, pharmaceutical, and psychosocial interventions. Firstly, psychosocial approaches (Table 2) investigate approaches such as counselling as well as attitudinal and behavioural therapies to assist in vaping cessation. Furthermore, these approaches also consider the involvement of the youths' communities (e.g. families and peers).

Table 2. Psychosocial Interventions

Interventions	Summary
Counselling (Hadland & Chadi, 2020)	Counselling is recommended utilising a framework that is youth-focused and a strength-based approach to work with youth vapers.
Vaping Cessation Text Message – This Is Quitting (TIQ) Program (Graham et al., 2021)	The TIQ program is a tailored text message programme for youths, where messages involve social support, norms and practical skills individuals can use. Findings showed that participants were more likely to quit vaping by the 7-month.
Cognitive Behavioural Therapy Approaches through Social Media Posts (Lyu et al., 2022)	Vaping cessation intervention implemented on Instagram where individuals are assigned to groups and receive 3 posts per weekday. The posts involve cognitive behavioural therapy, commitments to quit, stimulus control, and counter-conditioning.
Vaping Cessation through CBT interventions with coaching and Nicotine-Replacement Therapy (Webb et al., 2023)	Using an application to deliver self-guided personalised Cognitive Behavioural Therapy content along with nicotine replacement therapy involving nicotine gum/ patches. The study showed that this treatment was effective in addressing vaping prevalence.
Motivational Interviewing for E-cigarette cessation delivered through telehealth along with nicotine replacement therapy (Steinberg et al., 2022)	Participants received four weekly sessions of motivational interviewing via telehealth along with nicotine patches which was effective in participant's abstaining from vapes.

Environmental interventions refer to changes made to the vaper's social circumstances, external cues, or introduction of incentives to deter vaping (Table 3). The majority of these programmes focus on utilising a replacement for vaping products such as patches and lozenges. The programmes also consist of interventions designed to target the physical environment that youths interact with to nudge them towards non-vaping behaviour.

Table 3. Environmental Interventions

Intervention	Summary
Utilising Message Elements (Boynton et al., 2023)	Uses message elements that resonate with youths such as chemical constituents and health consequences. Recommends avoiding the usage of messaging referencing flavours or norms.
Behavioural Intervention for Vaping Cessation via Telehealth (Palmer et al., 2022)	Contingency management delivered digitally where incentives are provided contingent to abstinence after the quit date. The study was effective where the treatment was favoured, and 55% of the participants submitted abstinent samples.
Nicotine Replacement Therapy (Silver et al., 2016)	Utilising nicotine patches and lozenges in place of vapes as well as behavioural change strategies for six months allowed the sample population to remain vape-free, more than a year after quitting.
Nicotine Replacement Therapy (Palmer et al., 2023)	Utilising nicotine patches and lozenges along with a supportive booklet/Quitline referral. The study found that six vape users reported abstinence from vaping.

Singapore could consider combining the interventions (e.g. environmental, pharmaceutical, and psychosocial) which could help enhance the effectiveness of interventions available for vape cessation (Eisenberg et al., 2020).

RECOMMENDATIONS

This article has examined the risk and protective factors associated with vaping from a biopsychosocial lens to provide a more holistic view of the phenomenon of youth vaping. From the review, risk factors identified include demographics, personality, traumatic/adverse childhood experiences, outcome expectancies, psychological constructs such as anxiety sensitivity and curiosity, as well as cultural norms, peer influences and the attributes and marketing of vape products. Some protective factors found to reduce the risk of vaping are beliefs about vaping, internal development, normative beliefs, parental influences, and spirituality. We also looked at the prevention education efforts and cessation interventions available in Singapore and globally and evaluated the utility of vaping as a harm reduction tool from available research.

There are numerous studies accounting for the myriad of risk factors increasing susceptibility of vape usage among youths. However, we need a better understanding of the protective factors that can help to deter youth vaping to develop better strength-based interventions. Due to vapes being illegally marketed in Singapore through online retailing and the use of flavourings, policies targeting these components should be more stringent, to increase enforcement. More international collaborations with countries geographically nearer to Singapore should be considered to implement mutually beneficial policies that could aid in curbing importation of vapes to Singapore. Suggestions from interventions conducted in other countries could be considered to enhance current prevention programmes in Singapore.

ABOUT THE AUTHORS

Leung Chi Ching
is Lead Psychologist with the Home Team Psychology Division at the Ministry of Home Affairs, Singapore. She graduated from the Singapore Management University and obtained her doctorate in psychology from the National University of Singapore. She manages the drug portfolio within the division, looking into understanding drug abuse and addiction from the psychological perspective. Her research interest lies in the application of positive psychology to criminology and addiction.

Sherrer See
graduated from Temasek Polytechnic and was an intern with the Home Team Psychology Division at the Ministry of Home Affairs, Singapore under the supervision of Chi Ching. She is passionate about research and had the opportunity to research areas such as drug abuse as well as read on related topics such as the biopsychosocial model during her internship. Her personal observations of social trends among young people led her to initiate the idea of conducting a literature review on the harms of vaping.

The Home Team Psychology Division (HTPD) provides support to the Ministry of Home Affairs (MHA) and Home Team Departments (HTDs) by applying psychological sciences and conducting research to support policy development and enhance operations. HTPD also supports and develops psychologists across the various HTDs.

Established as a division within MHA on 1 Feb 2023 following the merger of the Home Team Behavioural Sciences Centre, Office of Chief Psychologist and Centre for Advanced Psychological Sciences, HTPD conducts research to improve outcomes in areas such as:

a. Forensic and criminal psychology, e.g. related to scams, drugs and sexual offending
b. Leadership assessment and talent development psychology
c. Crisis preparedness and community safety and security
d. Communication and information psychology
d. Mental resilience and well-being of our Home Team officers

HTPD uses behavioural sciences to support Home Team officers, to ensure they are operationally ready. This includes conducting regular mental health surveys to track stress levels, and providing standards and research into managing fatigue and building resilience and peer support. HTPD has also conducted research to examine the integration of physiological, mental, and emotional responses to better prepare our officers for the work they do.

HTPD also works closely as a community of psychologists in the Home Team, to support professional development and develop standardised practices. HTPD does this through organising and conducting workshops for our psychologists; and putting in place programmes to support the growth of the team.

REFERENCES

Ahmed, L. A., Verlinden, M., Alobeidli, M. A., Alahbabi, R. H., Alkatheeri, R., Saddik, B., Oulhaj, A., & Al-Rifai, R. H. (2021). Patterns of Tobacco Smoking and Nicotine Vaping among University Students in the United Arab Emirates: A Cross-Sectional Study. *International Journal of Environmental Research and Public Health, 18*(14), 7652. https://doi.org/10.3390/ijerph18147652

Ainslie, G. (1975). Specious reward: A behavioral theory of impulsiveness and impulse control. *Psychological Bulletin, 82*(4), 463–496. https://doi.org/10.1037/h0076860

Amin, S., Dunn, A. G., & Laranjo, L. (2020). Social Influence in the Uptake and Use of Electronic Cigarettes: A Systematic review. *American Journal of Preventive Medicine, 58*(1), 129–141. https://doi.org/10.1016/j.amepre.2019.08.023

Anand, K. S., & Dhikav, V. (2012). Hippocampus in health and disease: An overview. *Annals of Indian Academy of Neurology, 15*(4), 239. https://doi.org/10.4103/0972-2327.104323

Ang, S. (2023). Commentary: Is it time for vaping cessation programmes in Singapore? *CNA*. https://www.channelnewsasia.com/commentary/vaping-ecigarette-smoking-cessation-nicotine-free-quitting-programme-3591961

Asdigian, N. L., Riggs, N. R., Valverde, P., & Crane, L. A. (2022). Reducing Youth vaping: A pilot test of the Peer-Led "Youth Engaged Strategies for Changing Adolescent Norms!" (YES-CAN!) program. *Health Promotion Practice, 24*(5), 956–962. https://doi.org/10.1177/15248399221100793

Augenstein, J. A., Smaldone, A., Usseglio, J., & Bruzzese, J. (2024). Electronic Cigarette use and academic performance among Adolescents and young Adults: A scoping review. *Academic Pediatrics, 24*(2), 228–242. https://doi.org/10.1016/j.acap.2023.09.012

Bandura, A. (1977). Self-efficacy: Toward a unifying theory of behavioural change. *Psychological Review, 84*(2), 191-215.

Banks, E., Yazidjoglou, A., Brown, S., Ford, L., Zulfiqar, T., Baenziger, O., & Joshy, G. (2020). Systematic review and meta-analysis of evidence on the efficacy of e-cigarette use for sustained smoking and nicotine cessation. *medRxiv* (Cold Spring Harbor Laboratory). https://doi.org/10.1101/2020.11.02.20224212

Barrington-Trimis, J. L., Berhane, K., Unger, J. B., Cruz, T. B., Huh, J., Leventhal, A. M., Urman, R., Wang, K., Howland, S., Gilreath, T. D., Chou, C., Pentz, M. A., & McConnell, R. (2015). Psychosocial factors associated with adolescent electronic cigarette and cigarette use. *Pediatrics, 136*(2), 308–317. https://doi.org/10.1542/peds.2015-0639

Baker, J.A., Ang, H.M. (2021). Illegal vape devices and accessories sold openly on messaging apps, social media platforms. CNA. https://www.channelnewsasia.com/singapore/buy-vape-on-telegram-in-singapore-illegal-vapehouse-sgvape-282261

Barker, J., Kelley, D., Noar, S. M., Reboussin, B. A., Ross, J. C., & Sutfin, E. L. (2019). E-Cigarette Outcome Expectancies among Nationally Representative Samples of Adolescents and Young Adults. *Substance Use & Misuse, 54*(12), 1970–1979. https://doi.org/10.1080/10826084.2019.1624773

Becker, T., & Rice, T. (2021). Youth vaping: a review and update on global epidemiology, physical and behavioral health risks, and clinical considerations. *European Journal of Pediatrics, 181*(2), 453–462. https://doi.org/10.1007/s00431-021-04220-x

Berg, C. J., Melena, A., Wittman, F. D., Robles, T., & Henriksen, L. (2022). The reshaping of the E-Cigarette retail environment: its evolution and public health concerns. *International Journal of Environmental Research and Public Health, 19*(14), 8518. https://doi.org/10.3390/ijerph19148518

Boynton, M. H., Sanzo, N., Brothers, W., Kresovich, A., Sutfin, E. L., Sheeran, P., & Noar, S. M. (2023). Perceived effectiveness of objective elements of vaping prevention messages among adolescents. *Tobacco Control*, 32: e228-e235.

Burrowes, K. S., Fuge, C., Murray, T., Amos, J., Pitama, S., & Beckert, L. (2022). An evaluation of a New Zealand "vape to quit smoking" program. *New Zealand Medical Journal, 135*(1561).

Carrió, F. B. (2004). The Biopsychosocial model 25 years later: Principles, practice, and scientific inquiry. *Annals of Family Medicine, 2*(6), 576–582. https://doi.org/10.1370/afm.245

Cartujano-Barrera, F., Azogini, C., McIntosh, S., Bansal-Travers, M., Ossip, D. J., & Cupertino, A. P. (2021). Developing graphic messages for vaping prevention among Black and Latino Adolescents: Participatory Research approach. *Journal of Participatory Medicine, 13*(3), e29945. https://doi.org/10.2196/29945

CNA. (2023). The Big Read: With vaping increasingly rampant among youths despite ban, what more can authorities do? CNA. https://www.channelnewsasia.com/singapore/vaping-youths-cigarettes-legalise-vape-regulate-smoke-3419681

CNA. (2024). 65 vapes suspected to contain cannabis compound seized during drug raids. CNA. https://www.channelnewsasia.com/singapore/weed-cannabis-vape-thc-cnb-drug-raid-arrest-4246981

Choi, H. J., Miller-Day, M., Hecht, M. L., Glenn, S. D., Lyons, R., & Greene, K. (2022). A snapshot of parenting practices useful for preventing adolescent vaping. *Addictive Behaviors Reports, 15*, 100418. https://doi.org/10.1016/j.abrep.2022.100418

Christakis, N. A., & Fowler, J. H. (2008). The collective dynamics of smoking in a large social network. *The New England Journal of Medicine, 358*(21), 2249–2258. https://doi.org/10.1056/nejmsa0706154

Codd, L., Blackmore, D. G., Vukovic, J., & Bartlett, P. F. (2020). Exercise reverses learning deficits induced by hippocampal injury by promoting neurogenesis. *Scientific Reports, 10*(1). https://doi.org/10.1038/s41598-020-76176-1

Coleman, B., Apelberg, B. J., Ambrose, B. K., Green, K. M., Choinière, C. J., Bunnell, R., & King, B. A. (2014). Association between electronic cigarette use and openness to cigarette smoking among US young adults. *Nicotine & Tobacco Research, 17*(2), 212–218. https://doi.org/10.1093/ntr/ntu211

Conway, K. P., Green, V. R., Kasza, K. A., Silveira, M. L., Borek, N., Kimmel, H. L., Sargent, J. D., Stanton, C. A., Lambert, E., Hilmi, N., Reissig, C. J., Jackson, K. J., Tanski, S. E., Maklan, D., Hyland, A., & Compton, W. M. (2018). Co-occurrence of tobacco product use, substance use, and mental health problems among youth: Findings from wave 1 (2013–2014) of the population assessment of tobacco and health (PATH) study. *Addictive Behaviors, 76*, 208–217. https://doi.org/10.1016/j.addbeh.2017.08.009

Cooney, S. M., Huser, M., Small, S., & Connor, C. (2007). Evidence-based programs: An overview. What works, Wisconsin- Research to Practice Series. University of Wisconsin-Madison and University of Wisconsin-Extension, 6. https://fyi.extension.wisc.edu/whatworkswisconsin/files/2014/04/whatworks_06.pdf

Davey, M. (2022). 'I've lost my children to vaping': the tragic stories behind the soaring rates of youth addiction. *The Guardian*. https://www.theguardian.com/australia-news/2022/dec/02/ive-lost-my-children-to-vaping-the-tragic-stories-behind-the-soaring-rates-of-youth-addiction

De Vries, H., Backbier, E., Kok, G., & Dijkstra, M. (1995). The impact of social influences in the context of Attitude, Self-Efficacy, Intention, and previous behavior as predictors of smoking onset1. *Journal of Applied Social Psychology, 25*(3), 237–257. https://doi.org/10.1111/j.1559-1816.1995.tb01593.x

Dishion, T. J., & McMahon, R. J. (1998). Parental monitoring and the prevention of child and adolescent problem behavior: A conceptual and empirical foundation. *Clinical Child and Family Psychology Review, 1*(1), 61–75.

Donaldson, E. A., Hoffman, A. C., Zandberg, I., & Blake, K. D. (2017). Media exposure and tobacco product addiction beliefs: Findings from the 2015 Health Information National Trends Survey (HINTS–FDA 2015). *Addictive Behaviors, 72*, 106–113. https://doi.org/10.1016/j.addbeh.2017.04.001

Donaldson, C. D., Stupplebeen, D. A., Fecho, C. L., Ta, T., Zhang, X., & Williams, R. J. (2022). Nicotine vaping for relaxation and coping: Race/ethnicity differences and social connectedness mechanisms. *Addictive Behaviors, 132*, 107365. https://doi.org/10.1016/j.addbeh.2022.107365

Durkin, K., Williford, D. N., Turiano, N. A., Blank, M. D., Enlow, P. T., Murray, P. J., Banvard-Fox, C., & Duncan, C. L. (2020). Associations between peer use, costs and benefits, Self-Efficacy, and adolescent e-cigarette use. Journal of Pediatric Psychology, 46(1), 112–122. https://doi.org/10.1093/jpepsy/jsaa097

East, K., Hitchman, S. C., Bakolis, I., Williams, S., Cheeseman, H., Arnott, D., & McNeill, A. (2018). The association between smoking and electronic cigarette use in a cohort of young people. *Journal of Adolescent Health, 62*(5), 539–547. https://doi.org/10.1016/j.jadohealth.2017.11.301

Eisenberg, M. J., Hébert-Losier, A., Windle, S. B., Greenspoon, T., Brandys, T., Fülöp, T., Nguyen, T., Elkouri, S., Montigny, M., Wilderman, I., Bertrand, O., Bostwick, J., Abrahamson, J., Lacasse, Y., Pakhalé, S., Cabaussel, J., Filion, K. B., & Investigators, E. S. (2020). Effect of e-Cigarettes Plus Counseling vs Counseling Alone on Smoking Cessation. *JAMA, 324*(18), 1844. https://doi.org/10.1001/jama.2020.18889

Engel, G. L. (1977). The need for a new medical model: a challenge for biomedicine. *Science, 196*(4286), 129–136. https://doi.org/10.1126/science.847460

Erhabor, J., Boakye, E., Osuji, N., Obisesan, O. H., Osei, A. D., Mirbolouk, H., Stokes, A., Dzaye, O., El-Shahawy, O., Rodríguez, C. J., Hirsch, G. A., Benjamin, E. J., DeFilippis, A. P., Robertson, R. M., Bhatnagar, A., & Blaha, M. J. (2023). Psychosocial stressors and current e-cigarette use in the youth risk behavior survey. *BMC Public Health, 23*(1). https://doi.org/10.1186/s12889-023-16031-w

Erku, D. A., Gartner, C., Morphett, K., Snoswell, C. L., & Steadman, K. J. (2020). Nicotine vaping products as a harm reduction tool among smokers: Review of evidence and implications for pharmacy practice. *Research in Social and Administrative Pharmacy, 16*(9), 1272–1278. https://doi.org/10.1016/j.sapharm.2020.02.002

Fite, P. J., Cushing, C. C., Poquiz, J. L., & Frazer, A. L. (2018). Family influences on the use of e-cigarettes. *Journal of Substance Use, 23*(4), 396–401. https://doi.org/10.1080/14659891.2018.1436601

Foster, C. E., Horwitz, A. G., Thomas, A., Opperman, K. J., Gipson, P. Y., Burnside, A., Stone, D. M., & King, C. A. (2017). Connectedness to family, school, peers, and community in socially vulnerable adolescents. *Children and Youth Services Review, 81*, 321–331. https://doi.org/10.1016/j.childyouth.2017.08.011

Garey, L., Smit, T., Mayorga, N. A., Peraza, N., Nizio, P., Otto, M. W., & Zvolensky, M. J. (2019). Differential Effects of anxiety sensitivity on E-Cigarettes processes: The Importance of E-Cigarette Quit Attempt history. *The American Journal on Addictions, 28*(5), 390–397. https://doi.org/10.1111/ajad.12940

Gilmore, B.A., Gilmore, C.M., Reveles, K.R., Koeller, J.M., Spoor, J.H., Flores, B.E., & Frei, C.R. (2023). A Survey of Vaping Use, Perceptions, and Access in Adolescents from South-Central Texas Schools. International Journal of Environmental Research and Public Health, 20.

Giroud, C., De Cesare, M., Berthet, A., Varlet, V., Concha-Lozano, N., & Favrat, B. (2015). E-Cigarettes: A review of new trends in cannabis use. International Journal of Environmental *Research and Public Health/International Journal of Environmental Research and Public Health, 12*(8), 9988–10008. https://doi.org/10.3390/ijerph120809988

Goldenson, N. I., Leventhal, A. M., Simpson, K., & Barrington-Trimis, J. L. (2019). A review of the use and appeal of flavored electronic cigarettes. *Current Addiction Reports, 6*(2), 98–113. https://doi.org/10.1007/s40429-019-00244-4

Goriounova, N. A., & Mansvelder, H. D. (2012). Short- and Long-Term Consequences of Nicotine Exposure during Adolescence for Prefrontal Cortex Neuronal Network Function. *Cold Spring Harbor Perspectives in Medicine, 2*(12), a012120. https://doi.org/10.1101/cshperspect.a012120

Graham, A. L., Amato, M. S., Cha, S., Jacobs, M. A., Bottcher, M. M., & Papandonatos, G. D. (2021). Effectiveness of a vaping cessation text message program among young adult e-Cigarette users. *JAMA Internal Medicine*. https://doi.org/10.1001/jamainternmed.2021.1793

Grant, J. E., Lust, K., Fridberg, D. J., King, A. C., & Chamberlain, S. R. (2019). E-cigarette use (vaping) is associated with illicit drug use, mental health problems, and impulsivity in university students. *Ann Clin Psychiatry, 31*(1):27-35. PMID: 30699215; PMCID: PMC6420081.

Griffiths, M. A., Harmon-Kizer, T. R., & Gilly, M. C. (2011). Hubble Bubble Trouble: The Need for Education about and Regulation of Hookah Smoking. *Journal of Public Policy & Marketing, 30*(1), 119–132. https://doi.org/10.1509/jppm.30.1.119

Groom, A., Vu, T. H. T., Landry, R. L., Kesh, A., Hart, J. L., Walker, K. L., Wood, L. A., Robertson, R. M., & Payne, T. J. (2021). The Influence of Friends on Teen Vaping: A Mixed-Methods approach. *International Journal of Environmental Research and Public Health, 18*(13), 6784. https://doi.org/10.3390/ijerph18136784

Grossman, E. J., & Inglese, M. (2016). The role of thalamic damage in mild traumatic brain injury. *Journal of Neurotrauma, 33*(2), 163–167. https://doi.org/10.1089/neu.2015.3965

Hadland, S. E., & Chadi, N. (2020). Through the Haze: What clinicians can do to address youth vaping. *Journal of Adolescent Health, 66*(1), 10–14. https://doi.org/10.1016/j.jadohealth.2019.10.009

Hamberger, E., & Halpern-Felsher, B. (2020). Vaping in adolescents. *Current Opinion in Pediatrics, 32*(3), 378–383. https://doi.org/10.1097/mop.0000000000000896

Hartmann-Boyce, J., Lindson, N., Butler, A. R., McRobbie, H., Bullen, C., Begh, R., Theodoulou, A., Notley, C., Rigotti, N. A., Turner, T., Fanshawe, T., & Hájek, P. (2022). Electronic cigarettes for smoking cessation. *The Cochrane Library, 2023*(3). https://doi.org/10.1002/14651858.cd010216.pub7

Health Promotion Board. (2024). Secondary Schools and JCs. Health Promotion Board. https://hpb.gov.sg/schools/school-programmes/health-promoting-programmes-for-secondary-schools-and-jcs

Heldt, N. A., Seliga, A., Winfield, M., Gajghate, S., Reichenbach, N. L., Xiang, Y., Rom, S., Tenneti, A., May, D., Gregory, B. D., & Persidsky, Y. (2020). Electronic cigarette exposure disrupts blood-brain barrier integrity and promotes neuroinflammation. *Brain Behavior and Immunity, 88*, 363–380. https://doi.org/10.1016/j.bbi.2020.03.034

Hill, T. D., Bostean, G., Upenieks, L., Bartkowski, J. P., Ellison, C. G., & Burdette, A. M. (2022). (Un)holy Smokes? Religion and Traditional and E-Cigarette Use in the United States. *Journal of Religion and Health, 63*(2), 1334–1359. https://doi.org/10.1007/s10943-022-01721-3

Holtermann, C. (2023). E-cigarettes get a Gen-Z makeover. *The New York Times*. https://www.nytimes.com/2023/11/06/style/vape-elf-bar-juul.html

Honeycutt, L., Huerne, K., Miller, A., Wennberg, E., Filion, K. B., Grad, R., Gershon, A. S., Ells, C., Gore, G., Benedetti, A., Thombs, B. D., & Eisenberg, M. J. (2022). A systematic review of the effects of e-cigarette use on lung function. *Npj Primary Care Respiratory Medicine, 32*(1). https://doi.org/10.1038/s41533-022-00311-w

Hussain, M., Walker, C., & Moon, G. (2017). Smoking and Religion: Untangling Associations using English Survey data. *Journal of Religion & Health, 58*(6), 2263–2276. https://doi.org/10.1007/s10943-017-0434-9

Jackson, D. B., Boccio, C. M., Leal, W. E., & Vaughn, M. G. (2019). It's all the rage! Exploring the nuances in the link between vaping and adolescent delinquency. *Journal of Criminal Justice, 63*, 58–69. https://doi.org/10.1016/j.jcrimjus.2019.04.004

Jacobsen, L. K., Krystal, J. H., Mencl, W. E., Westerveld, M., Frost, S. J., & Pugh, K. R. (2005). Effects of smoking and smoking abstinence on cognition in adolescent tobacco smokers. *Biological Psychiatry, 57*(1), 56–66. https://doi.org/10.1016/j.biopsych.2004.10.022

Javed, S., Usmani, S., Sarfraz, Z., Sarfraz, A., Hanif, A., Firoz, A., Baig, R., Sharath, M., Walia, N., Chérrez-Ojeda, I., & Ahmed, S. (2022). A scoping review of vaping, E-Cigarettes and Mental Health Impact: Depression and Suicidality. *Journal of Community Hospital Internal Medicine Perspectives., 12*(3), 33–39. https://doi.org/10.55729/2000-9666.1053

Jerusalem, M., & Hessling, J. K. (2009). Mental health promotion in schools by strengthening self-efficacy. *Health Education, 109*(4), 329–341. https://doi.org/10.1108/09654280910970901

Johnson, S., Blum, R. W., & Cheng, T. L. (2016). Future orientation: a construct with implications for adolescent health and wellbeing. *International Journal of Adolescent Medicine and Health, 26*(4), 459–468. https://doi.org/10.1515/ijamh-2013-0333

Jonas, A. (2022). Impact of vaping on respiratory health. BMJ, e065997. https://doi.org/10.1136/bmj-2021-065997
Jones, R., Asare, M., & Lanning, B. A. (2020). A retrospective Cross-Sectional Study on the prevalence of e-cigarette use among college students. *Journal of Community Health, 46*(1), 195–202. https://doi.org/10.1007/s10900-020-00869-x

Jones, K., & Salzman, G. A. (2020). The Vaping Epidemic in Adolescents. *Missouri medicine, 117*(1), 56–58.

Kaleta, D., Wojtysiak, P., & Polańska, K. (2016). Use of electronic cigarettes among secondary and high school students from a socially disadvantaged rural area in Poland. *BMC Public Health, 16*(1). https://doi.org/10.1186/s12889-016-3417-y

Kaplan, R. C., Bangdiwala, S. I., Barnhart, J., Castañeda, S. F., Gellman, M. D., Lee, D. H., Pérez-Stable, E. J., Talavera, G. A., Youngblood, M., & Giachello, A. L. (2014). Smoking among U.S. Hispanic/Latino adults. *American Journal of Preventive Medicine, 46*(5), 496–506. https://doi.org/10.1016/j.amepre.2014.01.014

Katz, S. J., Erkinnen, M., Lindgren, B. R., & Hatsukami, D. K. (2019). Beliefs about E-cigarettes: A Focus Group Study with College Students. *American Journal of Health Behavior, 43*(1), 76–87. https://doi.org/10.5993/ajhb.43.1.7

Kelder, S. H., Mantey, D. S., Van Dusen, D., Case, K., Haas, A., & Springer, A. E. (2020). A middle school program to prevent E-Cigarette use: A pilot study of "CATCH My Breath." *Public Health Reports, 135*(2), 220–229. https://doi.org/10.1177/0033354919900887

Khouja, J. N., Wootton, R. E., Taylor, A. E., Smith, G. D., & Munafò, M. R. (2021). Association of genetic liability to smoking initiation with e-cigarette use in young adults: A cohort study. *PLOS Medicine, 18*(3), e1003555. https://doi.org/10.1371/journal.pmed.1003555

Kolb, B., & Whishaw, I. Q. (2003). *Fundamentals of human neuropsychology (5th ed.)*. Worth Publishers.

Kreski, N. T., Ankrum, H., Cerdá, M., Chen, Q., Hasin, D. S., Martins, S. S., Olfson, M., & Keyes, K. M. (2023). Nicotine Vaping and Co-occurring Substance Use Among Adolescents in the United States from 2017–2019. *Substance Use & Misuse, 58*(9), 1075–1079. https://doi.org/10.1080/10826084.2023.2188462

Krishnasamy, V., Hallowell, B. D., Ko, J. Y., Board, A., Hartnett, K. P., Salvatore, P. P., Danielson, M., Kite-Powell, A., Twentyman, E., Kim, L., Cyrus, A., Wallace, M., Melstrom, P., Haag, B., King, B. A., Briss, P., Jones, C. M., Pollack, L. A., Ellington, S. (2020). Update: Characteristics of a nationwide outbreak of e-cigarette, or vaping, Product Use–Associated Lung Injury — United States, August 2019–January 2020. *Morbidity and Mortality Weekly Report, 69*(3), 90–94. https://doi.org/10.15585/mmwr.mm6903e2

Kristjánsson, Á. L., Mann, M. J., & Sigfúsdóttir, I. D. (2015). Licit and Illicit Substance Use by Adolescent E-Cigarette Users Compared with Conventional Cigarette Smokers, Dual Users, and Nonusers. *Journal of Adolescent Health, 57*(5), 562–564. https://doi.org/10.1016/j.jadohealth.2015.07.014

Landry, R. L., Groom, A., Vu, T. H. T., Stokes, A., Berry, K. M., Kesh, A., Hart, J. L., Walker, K. L., Giachello, A. L., Sears, C. G., McGlasson, K. L., Tompkins, L. K., Mattingly, D. T., Robertson, R. M., & Payne, T. J. (2019). The role of flavors in vaping initiation and satisfaction among U.S. adults. *Addictive Behaviors, 99*, 106077. https://doi.org/10.1016/j.addbeh.2019.106077

Latimer, L. (2023). E-cigarette expectancies, consequences, and preferred quit strategies: Implications for interventions with college students. Senior Theses, Trinity College Digital Repository. https://digitalrepository.trincoll.edu/theses/1039

Lechner, W. V., Janssen, T., Kahler, C. W., Audrain-McGovern, J., & Leventhal, A. M. (2017). Bi-directional associations of electronic and combustible cigarette use onset patterns with depressive symptoms in adolescents. *Preventive Medicine, 96*, 73–78. https://doi.org/10.1016/j.ypmed.2016.12.034

Lee, A., Lee, K., & Park, H. (2019). Association of the Use of a Heated Tobacco Product with Perceived Stress, Physical Activity, and Internet Use in Korean Adolescents: A 2018 National Survey. *International Journal of Environmental Research and Public Health, 16*(6), 965. https://doi.org/10.3390/ijerph16060965

Lessard, J., Henrie, J., Livingston, J. A., Leonard, K. E., Colder, C. R., & Eiden, R. D. (2014). Correlates of ever having used electronic cigarettes among older adolescent children of alcoholic fathers. *Nicotine & Tobacco Research, 16*(12), 1656–1660. https://doi.org/10.1093/ntr/ntu148

Leslie, K. (2008). Harm reduction: An approach to reducing risky health behaviours in adolescents. *Paediatrics and Child Health, 13*(1), 53–56. https://doi.org/10.1093/pch/13.1.53

Ling, M. Y. J., Halim, A. F. N. A., Ahmad, D., Ahmad, N., Safian, N., & Nawi, A. M. (2023c). Prevalence and Associated Factors of E-Cigarette Use among Adolescents in Southeast Asia: A Systematic Review. *International Journal of Environmental Research and Public Health, 20*(5), 3883. https://doi.org/10.3390/ijerph20053883

Loh, F.F. (2023). Commentary: Malaysians losing battle on vaping after shock legalisation move. CNA. https://www.channelnewsasia.com/commentary/malaysia-vaping-legal-tax-youth-smoking-liquid-nicotine-poisons-list-3407901

Lyu, J. C., Olson, S. S., Ramo, D. E., & Ling, P. M. (2022). Delivering vaping cessation interventions to adolescents and young adults on Instagram: protocol for a randomised controlled trial. *BMC Public Health, 22*(1). https://doi.org/10.1186/s12889-022-14606-7

Lyzwinski, L. N., Naslund, J. A., Miller, C. J., & Eisenberg, M. J. (2022). Global youth vaping and respiratory health: epidemiology, interventions, and policies. *Npj Primary Care Respiratory Medicine, 32*(1). https://doi.org/10.1038/s41533-022-00277-9

Mai, J., Lin, L., Ling, Z., Guan, Q., Wang, Z., & Zhou, W. (2022). Will personality traits affect the use of e-cigar among college students? A cross-sectional study in Guangdong Province, China. *Frontiers in Public Health, 10*. https://doi.org/10.3389/fpubh.2022.1032606

Maiya, S., Whiteman, S. D., Serang, S., Dayley, J. C., Maggs, J. L., Mustillo, S., & Kelly, B. C. (2023). Associations between older siblings' substance use and younger siblings' substance use intentions: Indirect effects via substance use expectations. *Addictive Behaviors, 136*, 107493. https://doi.org/10.1016/j.addbeh.2022.107493

Manning, K., Mayorga, N. A., Garey, L., Kauffman, B. Y., Buckner, J. D., & Zvolensky, M. J. (2021). The Role of Anxiety Sensitivity and Fatigue Severity in Predicting E-Cigarette Dependence, Barriers to Cessation, and Cravings among Young Adults. *Substance Use & Misuse, 56*(13), 2059–2065. https://doi.org/10.1080/10826084.2021.1967990

Mantey, D. S., Clendennen, S. L., Springer, A. E., & Harrell, M. B. (2022). Perceived parental knowledge reduces risk for initiation of nicotine and cannabis vaping: a longitudinal study of adolescents. *American Journal of Health Promotion, 36*(4), 623–632. https://doi.org/10.1177/08901171211061941

Margolis, K. A., Nguyen, A. B., Slavit, W. I., & King, B. A. (2016). E-cigarette curiosity among U.S. middle and high school students: Findings from the 2014 national youth tobacco survey. *Preventive Medicine, 89*, 1–6. https://doi.org/10.1016/j.ypmed.2016.05.001

Marqués, P., Piqueras, L., & Sanz, M. (2021). An updated overview of e-cigarette impact on human health. *Respiratory Research, 22*(1). https://doi.org/10.1186/s12931-021-01737-5

Mayer, M., Reyes-Guzman, C., Grana, R., Choi, K., & Freedman, N. D. (2020). Demographic characteristics, cigarette smoking, and e-Cigarette use among US adults. *JAMA Network Open, 3*(10), e2020694. https://doi.org/10.1001/jamanetworkopen.2020.20694

Mayone, M., & Arneklev, B. J. (2015). Curiosity, Low Self-Control and Deviance: An Exploratory study. *Undergraduate Research Journal, 4*(1), 1. http://journals.fcla.edu/faurj/article/download/84470/81543

McCauley, D. M., Baiocchi, M., Cruse, S., & Halpern-Felsher, B. (2023). Effects of a short school-based vaping prevention program for high school students. *Preventive Medicine Reports, 33*, 102184. https://doi.org/10.1016/j.pmedr.2023.102184

McCashen, W. (2005). The Strengths Approach. St Luke's Innovative Resources. https://doi.org/10.1017/S1035077200011123

Meernik, C., Baker, H., Kowitt, S. D., Ranney, L. M., & Goldstein, A. O. (2019). Impact of non-menthol flavours in e-cigarettes on perceptions and use: an updated systematic review. *BMJ Open, 9*(10), e031598. https://doi.org/10.1136/bmjopen-2019-031598

Merrill, R. M., & Hanson, C. L. (2022). A formative evaluation of an adolescent online E-cigarette prevention program. *Health Education, 122*(6), 617–632. https://doi.org/10.1108/he-06-2021-0092

Milicic, S., DeCicca, P., Piérard, E., & Leatherdale, S. T. (2018). An evaluation of school-based e-cigarette control policies' impact on the use of vaping products. *Tobacco Induced Diseases, 16*(August). https://doi.org/10.18332/tid/93594

Minich, M., Falk, E. B., Cooper, N., Cosme, D., Chan, H., Pei, R., O'Donnell, M. B., & Cascio, C. N. (2023). Neural correlates associated with conformity in adolescent and young adult men. *Developmental Cognitive Neuroscience, 60*, 101215. https://doi.org/10.1016/j.dcn.2023.101215

Ministry of Culture, Community and Youth. (2021). Here for Youth. MCCY. https://www.mccy.gov.sg/sector/youth

Ministry of Health. (2024). Intensifying Enforcement and Education Efforts against E-vaporisers. Ministry of Health Singapore. https://www.moh.gov.sg/news-highlights/details/intensifying-enforcement-and-education-efforts-against-e-vaporisers#:~:text=In%202023%2C%207%2C838%20persons%20were,from%20the%204%2C916%20in%202022.

Mittal, A., Du, A. L., Merz, W., Myers, M. G., Alexander, L. E. C., & Doran, N. (2022). Impulsivity-Related Personality Traits as Predictors of E-Cigarette Use among Young Adults over Time. *Substance Use & Misuse, 57*(7), 1007–1013. https://doi.org/10.1080/10826084.2022.2046101

Moustafa, A. F., Rodriguez, D., Mazur, A., & Audrain-McGovern, J. (2021). Adolescent perceptions of E-cigarette use and vaping behavior before and after the EVALI outbreak. *Preventive Medicine, 145*, 106419. https://doi.org/10.1016/j.ypmed.2021.106419

Munafò, M. R., Zetteler, J., & Clark, T. G. (2007). Personality and smoking status: A meta-analysis. *Nicotine & Tobacco Research, 9*(3), 405–413. https://doi.org/10.1080/14622200701188851

National Institute of Environmental Health Sciences. (2023). Smoking and vaping. *National Institute of Environmental Health Sciences*. https://www.niehs.nih.gov/health/topics/agents/smoke/index.cfm

National Academies of Sciences, Engineering, and Medicine; Health and Medicine Division; Board on Population Health and Public Health Practice; Committee on the Review of the Health Effects of Electronic Nicotine Delivery Systems. (2018). Public Health Consequences of E-Cigarettes. Washington (DC): National Academies Press (US). Available from: https://www.ncbi.nlm.nih.gov/books/NBK507171/ doi: 10.17226/24952

National Academies of Sciences, Engineering, and Medicine; Division of Behavioral and Social Sciences and Education; Health and Medicine Division; Committee on Law and Justice; Board on Children, Youth, and Families; Board on Global Health; Forum on Global Violence Prevention. (2018). Addressing the Social and Cultural Norms That Underlie the Acceptance of Violence: Proceedings of a Workshop-in Brief. Washington (DC): National Academies Press (US). Available from: https://www.ncbi.nlm.nih.gov/books/NBK493719/ doi: 10.17226/25075

Neo, C.C., Tay, T. F. (2022). 'I can do it at home, the smell won't linger': Do youths who vape know what they are inhaling? CNA. 'I can do it at home, the smell won't linger': Do youths who vape know what they're inhaling? - CNA (channelnewsasia.com)

Ng, L., Ng, X. Y., & Van Der Eijk, Y. (2023). Vaping in a heavily regulated setting: cross-sectional survey of e-cigarette use, perceptions and social media exposure. *Tobacco Control, 33*(e1), e11–e17. https://doi.org/10.1136/tc-2022-057805

Nicksic, N. E., Harrell, M. B., Pérez, A., Pasch, K. E., & Perry, C. L. (2018). School policy, administrator perceptions, and student e-cigarette use. *Health Behavior and Policy Review, 5*(4), 72–82. https://doi.org/10.14485/hbpr.5.4.8

Noar, S. M., Gottfredson, N. C., Kieu, T., Rohde, J. A., Hall, M. G., Ma, H., Fendinger, N. J., & Brewer, N. T. (2022). Impact of vaping prevention advertisements on US adolescents. *JAMA Network Open, 5*(10), e2236370. https://doi.org/10.1001/jamanetworkopen.2022.36370

O'Dell, L. E. (2009). A psychobiological framework of the substrates that mediate nicotine use during adolescence. *Neuropharmacology, 56*, 263–278. https://doi.org/10.1016/j.neuropharm.2008.07.039

Oriakhi, M. (2020). Vaping: an emerging health hazard. Cureus. https://doi.org/10.7759/cureus.7421

Palmer, A., Tomko, R. L., Squeglia, L. M., Gray, K. M., Carpenter, M. J., Smith, T. T., Dahne, J., Toll, B. A., & McClure, E. A. (2022). A pilot feasibility study of a behavioral intervention for nicotine vaping cessation among young adults delivered via telehealth. *Drug and Alcohol Dependence, 232*, 109311. https://doi.org/10.1016/j.drugalcdep.2022.109311

Palmer, A., Carpenter, M. J., Rojewski, A. M., Haire, K., Baker, N. L., & Toll, B. A. (2023). Nicotine replacement therapy for vaping cessation among mono and dual users: A mixed methods preliminary study. *Addictive Behaviors, 139*, 107579. https://doi.org/10.1016/j.addbeh.2022.107579

Park, E., Kwon, M., Gaughan, M. R., Livingston, J. A., & Chang, Y. (2019). Listening to adolescents: their perceptions and information sources about e-cigarettes. *Journal of Pediatric Nursing, 48*, 82–91. https://doi.org/10.1016/j.pedn.2019.07.010

Patanavanich, R., Aekplakorn, W., Glantz, S. A., & Kalayasiri, R. (2021). Use of E-Cigarettes and Associated Factors among Youth in Thailand. *Asian Pacific Journal of Cancer Prevention, 22*(7), 2199–2207. https://doi.org/10.31557/apjcp.2021.22.7.2199

Patel, D. A., Davis, K., Cox, S., Bradfield, B., King, B. A., Shafer, P., Caraballo, R. S., & Bunnell, R. (2016). Reasons for current E -cigarette use among U.S. adults. *Preventive Medicine, 93*, 14–20. https://doi.org/10.1016/j.ypmed.2016.09.011

Pepper, J. K., Ribisl, K. M., & Brewer, N. T. (2016). Adolescents' interest in trying flavoured e-cigarettes. *Tobacco Control, 25*(Suppl 2), ii62–ii66. https://doi.org/10.1136/tobaccocontrol-2016-053174

Pettigrew, S., Santos, J. A., Li, Y., Jun, M., Anderson, C. S., & Jones, A. (2023). Short report: Factors contributing to young people's susceptibility to e-cigarettes in four countries. *Drug and Alcohol Dependence, 250*, 109944. https://doi.org/10.1016/j.drugalcdep.2023.109944

Pokhrel, P., Lam, T. H., Pagano, I., Kawamoto, C. T., & Herzog, T. A. (2018). Young adult e-cigarette use outcome expectancies: Validity of a revised scale and a short scale. *Addictive Behaviors, 78*, 193–199. https://doi.org/10.1016/j.addbeh.2017.11.019

Rebuli, M. E., Rose, J. J., Noël, A., Croft, D., Benowitz, N. L., Cohen, A. H., Goniewicz, M. Ł., Larsen, B. T., Leigh, N. J., McGraw, M. D., Melzer, A. C., Penn, A., Rahman, I., Upson, D., Alexander, L. E. C., Ewart, G., Jaspers, I., Jordt, S., Kligerman, S., . . . Witek, T. J. (2023). The e-cigarette or vaping product Use–Associated Lung Injury Epidemic: Pathogenesis, Management, and Future Directions: An Official American Thoracic Society Workshop report. *Annals of the American Thoracic Society, 20*(1), 1–17. https://doi.org/10.1513/annalsats.202209-796st

Reiss, S. (1987). Theoretical perspectives on the fear of anxiety. *Clinical Psychology Review, 7*(6), 585–596. https://doi.org/10.1016/0272-7358(87)90007-9

Reese, G., Rosenmann, A., & Cameron, J. E. (2019). *The psychology of globalization: Identity, ideology, and action*. Academic Press.

Reesor, L., Vaughan, E., Hernandez, D. C., & Johnston, C. A. (2017). Addressing outcomes expectancies in behavior change. *American Journal of Lifestyle Medicine, 11*(6), 430–432. https://doi.org/10.1177/1559827617722504

Ren, M., & Lotfipour, S. (2019). Nicotine gateway effects on adolescent substance use. the Western Journal of Emergency Medicine/Western *Journal of Emergency Medicine, 20*(5), 696–709. https://doi.org/10.5811/westjem.2019.7.41661

Rohde, J. A., Noar, S. M., Horvitz, C., Lazard, A. J., Ross, J. C., & Sutfin, E. L. (2018). The role of Knowledge and risk Beliefs in adolescent E-Cigarette Use: a pilot study. *International Journal of Environmental Research and Public Health, 15*(4), 830. https://doi.org/10.3390/ijerph15040830

Scheffels, J., Tokle, R., Linnansaari, A., Rasmussen, S. K. B., & Pisinger, C. (2023). E-cigarette use in global digital youth culture. A qualitative study of the social practices and meaning of vaping among 15–20-year-olds in Denmark, Finland, and Norway. *International Journal of Drug Policy, 111*, 103928. https://doi.org/10.1016/j.drugpo.2022.103928

Schwarzer, R., & Luszczynska, A. (2006). Self-efficacy, adolescents' risk-taking behaviours, and health. *Self-efficacy beliefs of adolescents, 5*, 139-159.

Scully, M., Greenhalgh, E., Bain, E., Wakefield, M., Durkin, S., & White, V. (2023). E-cigarette use and other risk factors associated with tobacco smoking susceptibility among Australian adolescents. *Australian and New Zealand Journal of Public Health, 47*(5), 100076. https://doi.org/10.1016/j.anzjph.2023.100076

Shang, C., Huang, J., Chaloupka, F. J., & Emery, S. (2017). The impact of flavour, device type and warning messages on youth preferences for electronic nicotine delivery systems: evidence from an online discrete choice experiment. *Tobacco Control, 27*(e2), e152–e159. https://doi.org/10.1136/tobaccocontrol-2017-053754

Shin, S. H., Conley, D. L., Jiskrova, G. K., & Wills, T. A. (2019). Adverse childhood experiences and E-Cigarette use during young adulthood. *The American Journal on Addictions, 28*(4), 303–310. https://doi.org/10.1111/ajad.12890

Shin, S. H. (2021). Preventing E-cigarette use among high-risk adolescents: A trauma-informed prevention approach. *Addictive Behaviors, 115*, 106795. https://doi.org/10.1016/j.addbeh.2020.106795

Silver, B., Ripley-Moffitt, C., Greyber, J., & Goldstein, A. O. (2016). Successful use of nicotine replacement therapy to quit e-cigarettes: lack of treatment protocol highlights need for guidelines. *Clinical Case Reports, 4*(4), 409–411. https://doi.org/10.1002/ccr3.477

Slomkowski, C., Rende, R., Novak, S. P., Lloyd-Richardson, E. E., & Niaura, R. (2005). Sibling effects on smoking in adolescence: evidence for social influence from a genetically informative design. *Addiction, 100*(4), 430–438. https://doi.org/10.1111/j.1360-0443.2004.00965.x

Soneji, S., Barrington-Trimis, J. L., Wills, T. A., Leventhal, A. M., Unger, J. B., Gibson, L., Yang, J. W., Primack, B. A., Andrews, J. A., Miech, R. A., Spindle, T. R., Dick, D. M., Eissenberg, T., Hornik, R., Dang, R., & Sargent, J. D. (2017). Association between initial use of e-Cigarettes and subsequent cigarette smoking among adolescents and young adults. *JAMA Pediatrics, 171*(8), 788. https://doi.org/10.1001/jamapediatrics.2017.1488

Stanford Medicine. (2022). Tobacco Prevention Toolkit. *Stanford Medicine*. https://med.stanford.edu/tobaccopreventiontoolkit.html

Statista. (2023). Demographics of Instagram users in Singapore as of June 2023, by age group. Statista. https://www.statista.com/statistics/1398467/singapore-demographics-of-instagram-users-by-age-group/

Statista. (2023). Distribution of Telegram users in 2023, by age group. Statista. https://www.statista.com/statistics/1252741/telegram-users-distribution-by-age-group/

Steinberg, M. L., Rosen, R., Ortiz, J. C., Billingsley, B., Steinberg, M. B., & Burnett, D. (2022). Motivational interviewing for e-cigarette cessation induction in young adults delivered via telehealth plus nicotine patch. *PsyArXiv Preprints*. https://doi.org/10.31234/osf.io/8z94j

Stratton, K., Kwan, L. Y., & Eaton, D. L. (2018). Public health consequences of E-Cigarettes. (2018). *In National Academies Press eBooks*. https://doi.org/10.17226/24952

Struik, L., Sharma, R., Rodberg, D., Christianson, K., & Lewis, S. (2023). A content analysis of behavior change techniques employed in North American vaping prevention interventions. *AJPM Focus, 2*(4), 100126. https://doi.org/10.1016/j.focus.2023.100126

Sun, D. (2023). Huge haul of 58,000 vapes found in cargo container in foiled smuggling bid. *The Straits Times*. https://www.straitstimes.com/singapore/huge-haul-of-58000-vapes-found-in-cargo-container-as-smuggling-attempt-foiled

Sutherland, B.D., Sutherland, M.T., & Trucco, E.M. (2022). Electronic Cigarette Use Intentions Mediate the Association between Low Self-Control and Future Use by Internalising Symptoms. *Substance Use & Misuse, 57*, 1797 - 1807.

Szoko, N., Ragavan, M. I., Khetarpal, S. K., Chu, K., & Culyba, A. J. (2021). Protective factors against vaping and other tobacco use. *Pediatrics, 148*(2). https://doi.org/10.1542/peds.2020-048066

Teah, G. E., & Conner, T. S. (2021). Psychological and demographic predictors of vaping and vaping susceptibility in young adults. *Frontiers in Psychology, 12*. https://doi.org/10.3389/fpsyg.2021.659206

Tehrani, H., Rajabi, A., Ghojogh, M. G., Nejatian, M., & Jafari, A. (2022). The prevalence of electronic cigarettes vaping globally: a systematic review and meta-analysis. *Archives of Public Health, 80*(1). https://doi.org/10.1186/s13690-022-00998-w

Tinner, L., Kelly, C., Caldwell, D., & Campbell, R. (2024). Community mobilisation approaches to preventing adolescent multiple risk behaviour: a realist review. *Systematic Reviews, 13*(1). https://doi.org/10.1186/s13643-024-02450-2

Tobacco (Control of advertisements and sale) act. (1993). https://sso.agc.gov.sg/Act/TCASA1993

Traboulsi, H., Cherian, M., Rjeili, M. A., Preteroti, M., Bourbeau, J., Smith, B. M., Eidelman, D. H., & Baglole, C. J. (2020). Inhalation toxicology of vaping products and implications for pulmonary health. *International Journal of Molecular Sciences, 21*(10), 3495. https://doi.org/10.3390/ijms21103495

Trivers, K. F., Watson, C., Neff, L. J., Jones, C. M., & Hacker, K. (2021). Tetrahydrocannabinol (THC)-containing e-cigarette, or vaping, product use behaviors among adults after the onset of the 2019 outbreak of e-cigarette, or vaping, product use-associated lung injury (EVALI). *Addictive Behaviors, 121*, 106990. https://doi.org/10.1016/j.addbeh.2021.106990

Trucco, E. M., Cristello, J. V., & Sutherland, M. T. (2021). Do parents still matter? The impact of parents and peers on adolescent electronic cigarette use. *Journal of Adolescent Health, 68*(4), 780–786. https://doi.org/10.1016/j.jadohealth.2020.12.002

Tushara, E. (2023). Vaping offences rise sharply in schools, enforcement and education being stepped up. *The Straits Times*. https://www.straitstimes.com/singapore/politics/vaping-offences-rise-sharply-in-schools-enforcement-and-education-being-stepped-up

United Nations. (n.d.). Definition of Youth. United Nations. http://undesadspd.org/Youth.aspx

Unger, J. B., Soto, D. W., & Leventhal, A. M. (2016). E-cigarette use and subsequent cigarette and marijuana use among Hispanic young adults. *Drug and Alcohol Dependence, 163*, 261–264. https://doi.org/10.1016/j.drugalcdep.2016.04.027

Van Der Eijk, Y. (2022). Commentary: Youth vaping too big a collateral damage to accept for a relatively ineffective smoking cessation aid. CNA. https://www.channelnewsasia.com/commentary/vaping-smoking-gateway-addiction-disease-youth-children-3027926

Van Der Eijk, Y., Ping, G. T. P., Ong, S. E., Xin, G. T. L., Li, D., Zhang, D., Shuen, L. M., & Seng, C. K. (2021). E-Cigarette markets and policy responses in Southeast Asia: A scoping review. *International Journal of Health Policy and Management*. https://doi.org/10.34172/ijhpm.2021.25

Vink, J. M., Willemsen, G., & Boomsma, D. I. (2005). Heritability of smoking initiation and nicotine dependence. *Behavior Genetics, 35*(4), 397–406. https://doi.org/10.1007/s10519-004-1327-8

Wamba, A., Pourchez, J., Julien, M. R., Christine, D., Leclerc, L., & Mabrouk, N. B. (2023). Impact of e-cigarette experimentation and use on smoking behavior among adolescents aged 15–16 years in the Loire department, France. *Tobacco Prevention and Cessation, 9*(June), 1–11. https://doi.org/10.18332/tpc/163416

Wawryk-Gawda, E., Lis-Sochocka, M., Chylińska-Wrzos, P., Budzyńska, B., & Jodłowska-Jędrych, B. (2019). The impact of traditional cigarettes and E-Cigarettes on the brain. In *Elsevier eBooks* (pp. 25–32). https://doi.org/10.1016/b978-0-12-813035-3.00004-6

Webb, J., Lin, Y., Ang, A., Michero, D., Majeed, A., Eisingerich, A. B., & Glasner, S. (2023). Feasibility and preliminary outcomes of a mobile intervention combining cognitive behavioral therapy, virtual coaching, and nicotine replacement therapy for nicotine vaping cessation. *Telemedicine Reports, 4*(1), 48–52. https://doi.org/10.1089/tmr.2023.0009

Weser, V., Duncan, L. R., Sands, B., Schartmann, A., Jacobo, S., François, B., & Hieftje, K. (2021). Evaluation of a virtual reality E-cigarette prevention game for adolescents. *Addictive Behaviors, 122*, 107027. https://doi.org/10.1016/j.addbeh.2021.107027

Whiteman, S. D., Jensen, A. C., Mustillo, S., & Maggs, J. L. (2016). Understanding sibling influence on adolescents' alcohol use: Social and cognitive pathways. *Addictive Behaviors, 53*, 1–6. https://doi.org/10.1016/j.addbeh.2015.09.007

Wilhelm, A. K., Parks, M. J., Eisenberg, M. E., & Allen, M. (2020). Patterns of tobacco use and related protective factors among Somali youth in the United States. *Journal of Immigrant and Minority Health, 23*(1), 103–112. https://doi.org/10.1007/s10903-020-01013-6

Williams, L., Clements-Nolle, K., Lensch, T., & Yang, W. (2020). Exposure to adverse childhood experiences and early initiation of electronic vapor product use among middle school students in Nevada. *Addictive Behaviors Reports, 11*, 100266. https://doi.org/10.1016/j.abrep.2020.100266

Wong, A. (2023). Giving up vaping for love: MacPherson Youth Network launches anti-vape campaign. *The Straits Times*. https://www.straitstimes.com/singapore/giving-up-vaping-for-love-macpherson-youth-network-launches-anti-vape-campaign

Xie, Z., Ossip, D. J., Rahman, I., O'Connor, R. J., & Li, D. (2020). Electronic cigarette use and subjective cognitive complaints in adults. *PloS One, 15*(11), e0241599. https://doi.org/10.1371/journal.pone.0241599

Yusoff, M. F. M., Riyadzi, M. R., Hamid, H. A. A., Lourdes, T. G. R., Saminathan, T. A., Lim, K. K. (2023). E-Cigarette use among adolescents in Malaysia: Findings from a National Survey. *Institute for Public Health, National Institutes of Health, Ministry of Health Malaysia*.

Zelikoff, J. T., Parmalee, N. L., Corbett, K., Gordon, T., Klein, C. B., & Aschner, M. (2017). Microglia activation and gene expression alteration of neurotrophins in the hippocampus following Early-Life exposure to E-Cigarette aerosols in a murine model. *Toxicological Sciences, 162*(1), 276–286. https://doi.org/10.1093/toxsci/kfx257

Zhong, S., Wang, Y., Chen, R., & Zhou, L. (2022). E-cigarette use among youth in China. *The Lancet Regional Health - Western Pacific, 24*, 100504. https://doi.org/10.1016/j.lanwpc.2022.100504

Zhou, P. J., Xia, W., Chen, R. Y., Leng, Y., Liu, T., & Sun, T. (2020). Prevalence and associated factors regarding electronic cigarette smoking among adults in Shandong province. *Chinese Journal of Epidemiology, 41*(10), 1681–1685. https://doi.org/10.3760/cma.j.cn112338-20191202-00847

PREVALENCE OF ILLICIT DRUG CONSUMPTION IN SINGAPORE:
FINDINGS OF THE SINGAPORE HEALTH AND LIFESTYLE SURVEY

Mythily Subramaniam, Koh Yen Sin, Rajeswari Sambasivam, Edimansyah Abdin, PV Asharani, Janhavi Ajit Vaingankar, Chua Boon Yiang, Chua Hong Choon, Lee Cheng, Chow Wai Leng, Stefan Ma, Chong Siow Ann
Institute of Mental Health, National University of Singapore, Nanyang Technological University, Khoo Teck Puat Hospital, Ministry of Health, Singapore

ABSTRACT

A nationwide population survey was undertaken from April 2021 to July 2022 to establish the prevalence of behavioural and substance addictions among those aged 15–65 years in Singapore. Involving a representative sample of 6,509 Singapore residents (i.e. Singapore citizens and permanent residents), it shows that those belonging to the younger age group, current and ex-smokers, as well as those with hazardous alcohol use, are at higher risk of lifetime consumption of drugs. These findings can help to inform healthcare workers, teachers and others who work with young people on illicit drug consumption in Singapore, as well as provide relevant data for policymaking. In particular, the study's finding that some 2.3% Singapore residents (more than 93,000 people) had consumed illicit drugs at least once in their lifetime – of which 28.9% (27,000 people) did so before they turned 18 years old—while 0.7% (28,300 people) had used illicit drugs in the past year—has implications for Singapore's drug prevention and early detection efforts.*

GLOBAL TRENDS IN SUBSTANCE ABUSE

Substance use disorders (SUDs) are characterised by the uncontrolled use of a substance by an individual despite its harmful consequences (American Psychiatric Association, 2013; Substance Abuse and Mental Health Services Administration [SAMHSA], 2020a). The prevalence of consumption of substances and SUDs varies widely across countries. This difference in prevalence can be attributed to factors such as study methodology (the substance included in the study, whether survey or administrative data were used), drug policies across countries, and the demographic and cultural profiles of the population.

According to the United Nations Office on Drugs and Crime (UNODC) World Drug Report, in 2020, an estimated 284 million people worldwide aged 15 to 64 (mostly men) had used an illicit drug within the last 12 months (UNODC, 2021). Of the people who had used drugs in the past year, about 13.6% suffered from SUDs (UNODC, 2021). The National Survey on Drug Use and Health (NSDUH) conducted annually in the US found that in 2021, 21.9% of people aged 12 or older (or 61.2 million people) used illicit drugs in the past year. Of these, 16.5% (46.3 million people) had an SUD as defined by the Diagnostic and Statistical Manual of Mental Disorders, Fifth Edition (DSM-5) in the past year (SAMHSA, 2020b). The European Monitoring Centre for Drugs and Drug

* This article is adapted from a paper by the authors published in the Annals, Academy of Medicine, Singapore, 2024;53:222-32, with the title, "Prevalence of Illicit Drugs Consumption and Associated Factors from a Nationwide Epidemiological Survey: The Singapore Health and Lifestyle Survey". The original paper can be read at https://annals.edu.sg/prevalence-of-consumption-of-illicit-drugs-and-associated-factors-from-a-nationwide-epidemiological-survey-the-singapore-health-and-lifestyle-survey/.

Addiction (EMCDDA) found that around 28.9% (83 million) of adults (aged 15 to 64) in the European Union had used illicit drugs at least once in their lifetime. In comparison, 7.7% (22.2 million) had used it in the past year (EMCDDA, 2021a).

On the other hand, data from Asian countries is limited. For example, a survey conducted in 2019 in India suggests that about 2.8% of the population had consumed cannabis products in the past year, while 2.1% used some form of opioids (Ambekar et al., 2019). In Hong Kong, data on illicit drug consumption is mainly from the Central Registry of Drug Abuse (Narcotics Division, Security Bureau, 2021). It shows that in 2021 there were 6,019 drug abusers. Among those reported, 2,388 or 41% were reported as heroin abusers, and 4,099 or 70% were reported as psychotropic substance abusers (Narcotics Division, Security Bureau, 2021).

Several sociodemographic factors have been associated with the consumption of substances. Younger males are significantly associated with a higher prevalence of consumption of substances (UNODC, 2021; Baptiste-Roberts & Hossain, 2018; Center for Behavioral Health Statistics and Quality; SAMHSA, 2015; SAMHSA, 2014). An Australian-New Zealand study examining the association between frequency of cannabis consumption before age 17 and high school noncompletion, university non-enrolment and degree non-attainment by age 25, found that adolescent cannabis consumption (weekly or more) was associated with 1.5 to 2-fold increases in the odds of high school noncompletion, university non-enrolment and degree non-attainment (Silins et al., 2015).

Individual, community- and country-level socioeconomic characteristics can directly or indirectly influence drug consumption. NSDUH found that among persons who reported lifetime use of illicit drugs, persons with a family income less than USD 20,000 were 36% more likely to report having substance use problems compared to those with a family income ≥ USD 75,000 (Baptiste-Roberts & Hossain, 2018).

Singapore's Arrest Data

Singapore takes a zero-tolerance stance against illicit drugs by adopting a comprehensive drug control strategy that tackles drug supply and demand. The multipronged strategy is spearheaded through preventive drug education; strict anti-drug laws; rigorous enforcement; international engagement and rehabilitation that includes treating, counselling and reintegrating drug offenders into society (Central Narcotics Bureau, 2023). However, information on the consumption of drugs in Singapore is limited to arrest data. According to statistics from the Central Narcotic Bureau (CNB), 2,826 drug abusers were arrested in 2022. Of these, about 28% (802) were new abusers. Methamphetamine (1,451), heroin (994) and cannabis (236) were the most commonly abused drugs (CNB, 2023).

However, no study has examined the prevalence of consumption of illicit drugs (i.e. the non-medical consumption of drugs prohibited by national law) in the Singapore general population. A study was thus undertaken by the authors to establish the lifetime (i.e. any consumption during the person's life) and 12-month (consumption in the last year) prevalence of illicit drug consumption and its socio-demographic and clinical correlates in the general population of Singapore.

THE SINGAPORE STUDY

Study Design

The Health and Lifestyle Survey is a nationwide population survey undertaken to establish the prevalence of behavioural and substance addictions among those aged 15–65 years in Singapore. Trained interviewers conducted the survey over 15 months, from April 2021 to July 2022.

Sample Size

The sample size for the study was calculated by conducting statistical power calculations for binary proportions to provide a precise estimate of a margin of error (MoE) equal to 0.05 for the overall and sub-groups. We assumed a statistical power of 0.80, with the Type 1 error at α=0.05. The design effect after oversampling by age and ethnicity was 1.765. As no local data on the prevalence rate of drug consumption could be used as a reference, we generated 2 power calculations based on an approximation of prevalence rates between 1% and 2%, respectively. In each calculation, we assumed specific, realistic sample sizes (e.g. n=5,500; 6,000; 6,500) and computed the MoE for key quantities of

interest. Using this approach, we determined that a sample size of 6,500 would provide sufficient precision to estimate 1-2% of drug consumption with a relative standard error of 11.5-16.4% and an MoE of 0.3-0.5% for the overall prevalence estimate.

Participants

A representative sample of Singapore residents (Singapore citizens and permanent residents) aged between 15 and 65 years were randomly selected from an administrative database. The inclusion criteria were that participants had to be Singapore residents, aged 15 to 65 years, belonging to any of the 4 ethnic groups in Singapore (Chinese, Malay, Indians and others), and literate in English, Chinese, Malay or Tamil. Exclusion criteria were (1) inability to complete the interview due to severe physical or mental health conditions, (2) illiteracy, (3) hospitalisation, or (4) institutionalisation lasting the entire duration of fieldwork.

Survey Methodology

A survey firm was employed to conduct the study, and respondents were approached by trained lay interviewers. Participants were sent an invitation letter and subsequently approached using door-knocks. A verbal consent was sought in person. If the participants were willing to participate in the study, a tablet with the survey was handed over to them to complete the questionnaires after the collection of basic sociodemographic data by the interviewer.

However, on 14 May 2021, the research team was informed of the need to suspend face-to-face recruitment due to the imposition of COVID-19-related restrictions. As a result, the team adopted a hybrid approach (face-to-face consent and online questionnaire) for all subsequent interviews. After getting the consent, the interviewers provided the participants with a QR code/hyperlink for accessing the survey as well as a unique code, which the participant had to key in to start the survey. The unique code prevented duplicate attempts or misuse of the link. Participants could not make any changes after submitting the survey.

Questionnaires

The European Model Questionnaire and the guidelines provided by EMCDDA for conducting population surveys of drug use were used to develop a questionnaire that assessed the lifetime and 12-month prevalence of drug consumption (EMCDDA 2002). Participants were asked about their consumption of illicit drugs – cannabis, heroin, cocaine, methamphetamine, ecstasy, ketamine, nimetazepam, buprenorphine, new psychoactive substances and prescription drugs (i.e. benzodiazepines / tranquilisers, sedatives / hypnotics / barbiturates and steroids) – in their lifetime and in the past year. Misuse of prescription drugs was established using two additional questions: (1) was this prescribed by a medical practitioner, and (2) did you take more than the prescribed dosage? All those who stated that they had ever consumed a drug (illicit or licit) in their lifetime were asked about their mode of drug consumption, age of initiation of drug consumption and reasons for taking drugs. They were also asked about the severity of drug consumption using a checklist based on the Diagnostic and Statistical Manual of Mental Disorders, Fourth Edition, Text Revision (DSM-IV-TR) criteria for substance use disorder. However, for this study, we focussed only on the drugs prohibited by national law in Singapore, i.e., cannabis, heroin, cocaine, methamphetamine, ecstasy, ketamine, nimetazepam, buprenorphine, new psychoactive substances, and not on the misuse of prescription drugs.

The Patient Health Questionnaire-9 was used to screen for the presence and severity of depression, while the Generalised Anxiety Disorder-7 (GAD-7) was used to screen for generalised anxiety disorder (Kroenke, Spitzer, & Williams, 2001; Spitzer et al., 2006). The Insomnia Severity Index was used to assess sleep problems (Morin et al., 2011). The Alcohol Use Disorders Identification Test was used to examine drinking habits and hazardous alcohol use (Saunders et al., 1993). Yes/No questions captured the smoking history, and participants were classified as current, past and never smokers based on their replies. The Chronic Medical Conditions Checklist captured doctor-diagnosed chronic physical conditions and a list of common mental illnesses in Singapore (Chong et al., 2012).

Information on the sociodemographic profile of the respondents, including age, gender, ethnicity, living circumstances, marital status and education level, were collected. Data on socioeconomic status (e.g. current occupational status, income and sources of income) were also obtained.

Ethical Considerations

Interviewers obtained verbal consent instead of signed written informed consent to prevent any documentation of the participants. Furthermore, no identifiers were collected to ensure that participants could not be linked to their data. A waiver of parental consent was requested and obtained from the institutional review board so that the minors would not feel apprehensive while answering the sensitive questions. All questions had response options, such as "I prefer not to answer" and "don't know" to allow participants to skip any question they felt was sensitive. Encrypted data from the interviews (without identifiers) were stored on the tablets and downloaded weekly by the survey firm to ensure complete confidentiality. Contact details of the respondents were not shared with the research team, and the survey firm destroyed all contact records three months after completion of the survey.

The National Healthcare Group Domain Specific Review Board (ethics committee) approved the study procedures and provided ethical approval.

SURVEY FINDINGS AND ANALYSIS

A total of 6,509 respondents were included in the analysis, with a response rate of 73.2%. The weighted mean age was at 40.9 (SD 14.2) years.[1] Slightly more individuals were aged 15 to 34 years old (36.3%, n=2404), female (50.8%, n=3353), had degree / professional / post-graduate and above qualification (36.4%, n=2035), and were married (57.7%, n=3839). The majority were of Chinese ethnicity (73.6%, n=2,130), employed / self-employed (75.8%, n=4709), and most had a personal income below SGD2,000 / No income (42.0%, n=2419). See Table 1.

Table 1. Sociodemographic Characteristics of the Sample

Age group	15 to 34	36.3% (2,404)
	35 to 49	31.3% (2,270)
	50 to 65	32.4% (1,835)
Gender	Female	50.8% (3,353)
	Male	49.2% (3,156)
Ethnicity	Chinese	73.6% (2,130)
	Malay	13.7% (2,162)
	Indian	9.2% (1,911)
	Others	3.5% (306)
Education	No formal education / Primary	7.4% (539)
	Secondary school	23.8% (1,555)
	Vocational institute / Institute of Technical Education / Pre-university / Junior college / Diploma / International baccalaureate	32.4% (2,289)
	Degree / Professional qualification and post-graduate and above	36.4% (2,035)
	Others	0.02% (3)
Marital status	Married	57.7% (3,839)
	Single	36.5% (2,202)
	Separated/Widowed/Divorced	5.8% (404)

[1]For information on how the sample data was weighted to adjust for the differential probability of the selection of respondents, non-response and post-stratified by age, gender and ethnicity between the survey sample and the Singapore resident population of 2020, see the original paper in the Annals, Academy of Medicine, Singapore, 2024;53:222-32

Employment	Employed/Self-employed	75.8% (4,709)
	Economically inactive/Students	20.6% (1,431)
	Unemployed/Temporarily laid off	3.6% (249)
	Others	0.06% (2)
Personal income	Below SGD2,000/No income	42.0% (2,419)
	SGD2,000 to SGD3,999	25.0% (1,441)
	SGD4,000 to SGD6,999	18.4% (818)
	SGD7,000 and above	14.6% (600)
Missing values: education (n=88), marital status (n=64), employment (n=118), personal income (n=1,231). Economically inactive includes housewives and retirees.		

Prevalence of Lifetime and Past 12-Month Illicit Drug Consumption

The lifetime prevalence of consuming illegal drugs was 2.3% (95% CI 1.9–2.8) (n=180). Among those who consumed illicit drugs in their lifetime, the mean age of onset was 19.6 years (SD 6.7), with 28.9% (n=35) consuming illegal drugs before reaching 18 years of age. The prevalence of lifetime illicit drug consumption was higher among those aged 15 to 34 years old (2.8%), males (2.9%), those belonging to other ethnicities (5.7%), with tertiary educational qualification (2.5%), separated/widowed/divorced (4.0%), those who were unemployed or temporarily laid off (4.5%), ex-smokers (7.5%) and those with hazardous alcohol use (9.7%). See Table 2.

Table 2. Sociodemographic Characteristics of the Sample Stratified by Lifetime Illicit Drug Consumed

	No illicit drug use (n=6,281)	Lifetime illicit drug use (n=180)	P value
Age group, no. (%)			**0.031**
15 to 34	97.2% (2,312)	2.8% (75)	
35 to 49	97.3% (2,198)	2.7% (62)	
50 to 65	98.6% (1,771)	1.4% (43)	
Gender, no. (%)			**0.012**
Female	98.3% (3,269)	1.7% (67)	
Male	97.1% (3,012)	2.9% (113)	
Ethnicity, no. (%)			**<0.001**
Chinese	98.1% (2,077)	1.9% (44)	
Malay	97.0% (2,080)	3.0% (62)	
Indian	96.9% (1,836)	3.1% (57)	
Others	94.3% (288)	5.7% (17)	
Education, no. (%)			**0.912**
No formal education/Primary	97.7% (517)	2.3% (14)	

Secondary school	98.0% (1,497)	2.0% (42)	
Vocational institute / Institute of Technical Education / Pre-university / Junior college / Diploma / International baccalaureate[+]	97.6% (2,213)	2.4% (61)	
Degree / Professional qualification and post-graduate and above	97.5% (1,971)	2.5% (60)	
Others	100% (3)	0% (0)	
Marital status, no. (%)			**0.222**
Married	97.9% (3,706)	2.1% (103)	
Single	97.7% (2,129)	2.3% (61)	
Separated/Widowed/Divorced	96.0% (386)	4.0% (14)	
Employment, no. (%)			**0.008**
Employed / Self-employed	97.3% (4,532)	2.7% (148)	
Economically inactive / Students	99.1% (1,401)	0.9% (20)	
Unemployed / Temporarily laid off	95.5% (235)	4.5% (12)	
Others	100% (2)	0% (0)	
Personal income, no. (%)			**0.316**
Below SGD2000/No income	98.0% (2,346)	2.0% (59)	
SGD2000–SGD3999	97.3% (1,385)	2.8% (49)	
SGD4000–SGD6999	97.6% (792)	2.4% (23)	
SGD7000 and above	96.5% (570)	3.5% (28)	
Smoking status, no. (%)			**<0.001**
Smoker	94.1% (941)	5.9% (72)	
Ex-smoker	92.5% (401)	7.5% (30)	
Non-smoker	98.7% (4,812)	1.3% (75)	
Hazardous alcohol use, no. (%)			**<0.001**
No	98.0% (5,553)	2.0% (138)	
Yes	90.3% (161)	9.7% (21)	

[#] Rao-Scott chi-square test was used to obtain P value.
[+] These are pre-tertiary educational qualifications.

Missing values: education (n for no drug use = 80, n for drug use = 3), marital status (n for no drug use = 60, n for drug use = 2), employment (n for no drug use = 111), personal income (n for no drug use = 1,188, n for drug use = 21), smoking status (n for no drug use = 127, n for drug use = 3), hazardous alcohol use (n for no drug use = 567, n for drug use = 23).

Economically inactive includes housewives and retirees.

The past 12-month illicit drug consumption prevalence was 0.7% (n=58). Given the low prevalence, no further analysis was done on this group. The prevalence of illicit drug abuse among those with illicit drug consumption was 23.3%, while that of drug dependence was 13.0% (using DSM-IV-TR criteria).

Table 3. First Drug Used and Most Frequent Drug Used (Top Three) Among Those Who Endorsed Lifetime Drug Consumption

	Weighted %	Unweighted frequency
What was the first drug that you have used? *		
Cannabis	82.8%	70
Methamphetamine	4.5%	7
Ecstasy	4.0%	3
Which drug did you use most frequently? #		
Cannabis	68.0%	45
Methamphetamine	15.5%	14
Heroin	6.5%	10

* 88 respondents with illicit drug use refused to answer this question or stated that they did not know.
# 105 respondents with illicit drug use refused to answer this question or stated that they did not know.

The First Drug Consumed and Most Frequently Consumed Illicit Drug

Cannabis was the most common drug that was first consumed (82.8%, n=70) in the lifetime, followed by methamphetamine (4.5%, n=7) and ecstasy (4.0%, n=3) (Table 3). Among the illicit drugs consumed in the lifetime, cannabis (68.0%, n=45), methamphetamine (15.5%, n=14) and heroin (6.5%, n=10) were most frequently consumed (Table 3).

Sociodemographic and Clinical Correlates of Lifetime Illicit Drug Consumption

Age, ethnicity, employment status, smoking status and hazardous alcohol use were significantly associated with lifetime drug consumption (Table 4). Compared to individuals aged 15 to 34, those aged 50 to 65 (OR 0.3, 95% CI 0.2–0.7) had lower odds of lifetime drug consumption. Smokers (OR 4.7, 95% CI 2.7–8.3) and ex-smokers (OR 5.9, 95% CI 3.2–11.1) were more likely to have lifetime drug consumption than non-smokers. Individuals with hazardous alcohol use (OR 3.3, 95% CI 1.7–6.5) had higher odds of lifetime drug consumption than those without hazardous alcohol use.

Table 4. Sociodemographic Correlates of Lifetime Illicit Drug Consumption

	OR (95% CI)	P value
Age group (in years)		
15 to 34 (Reference)		
35 to 49	0.7 (0.4–1.2)	0.208
50 to 65	0.3 (0.2–0.7)	0.005
Gender		
Female (Reference)		
Male	0.96 (0.6–1.6)	0.880

	OR (95% CI)	P value
Ethnicity		
Chinese (Reference)		
Malay	1.1 (0.7–1.9)	0.602
Indian	1.4 (0.9–2.2)	0.170
Others	2.1 (1.1–3.8)	0.023
Education		
Degree/Professional qualification and post-graduate and above (Reference)		
Secondary school	0.6 (0.3–1.3)	0.200
Institute of Technical Education / Vocational institute, pre-university / junior college, international baccalaureate	0.7 (0.4–1.3)	0.271
No formal education/Primary	0.8 (0.3–2.5)	0.711
Marital status		
Married (Reference)		
Single	0.8 (0.5–1.4)	0.519
Separated/Widowed/Divorced	1.9 (0.7–5.4)	0.210
Employment status		
Employed/Self-employed (Reference)		
Economically inactive/Students	0.4 (0.2–0.9)	0.032
Unemployed/Temporarily laid off	0.7 (0.4–1.5)	0.353
Smoking status		
Non-smoker (Reference)		
Smoker	4.7 (2.7–8.3)	<0.001
Ex-smoker	5.9 (3.2–11.1)	<0.001
Hazardous alcohol use		
No (Reference)		
Yes	3.3 (1.7–6.5)	0.001

Economically inactive includes housewives and retirees.
CI: confidence interval; OR: odds ratio.

Those with lifetime drug consumption had higher odds of having clinical anxiety (OR 2.2, 95% CI 1.1–4.6) and clinical insomnia (OR 2.0, 95% CI 1.2–3.4). Those with lifetime illicit drug consumption were more likely to report that a doctor had diagnosed them with depression or major depressive disorder (OR 4.1, 95% CI 2.0–8.6), bipolar disorder (OR 9.6, 95% CI 1.5–60.3), anxiety disorder (OR 3.4, 95% CI 1.4–8.1) and psychosis or schizophrenia (OR 8.8, 95% CI 1.4–56.3) (Table 5).

Table 5. Associations between Clinical Outcomes and Lifetime Illicit Drug Use

Clinical outcomes	OR (95% CI)	P value
Clinical Depression (PHQ-9)	1.5 (0.7–3.1)	0.273
Clinical Anxiety (GAD-7)	2.2 (1.1–4.6)	0.037
Clinical Insomnia (ISI)	2.0 (1.2–3.4)	0.013
Presence of chronic conditions (self-reported)	1.1 (0.7–1.6)	0.825
Depression or major depressive disorder (self-reported)	4.1 (2.0–8.6)	<0.001
Bipolar disorder (self-reported)	9.6 (1.5–60.3)	0.016
Anxiety disorder (self-reported)	3.4 (1.4–8.1)	0.006
Psychosis or Schizophrenia (self-reported)	8.8 (1.4–56.3)	0.022

Adjusted for age, ethnicity, employment status, smoking status and hazardous alcohol use.

Cut-off for various scales are as follows: PHQ-9 (≥10 for clinical depression), GAD-7 (≥10 for clinical anxiety), ISI (≥15).

CI: confidence interval; GAD-7: Generalised Anxiety Disorder -7; ISI: Insomnia Severity Scale; OR: odds ratio; PHQ-9: Patient Health Questionnaire-9.

IMPLICATIONS OF STUDY

This study is one of the first conducted in Singapore to examine the prevalence and correlates of illicit drug consumption. Its finding that the prevalence of lifetime and 12-month illicit drug consumption in the Singapore population was 2.3% and 0.7%, respectively, in 2021 is much lower than that reported in studies conducted in the US, Europe and Australia, which reported rates of 21.4% (in the past year), 28.9% (at least once in their lifetime) and 43% (at some point in their life), respectively (SAMHSA, 2020b; Australian Institute of Health and Welfare, 2020).

Still, given that the resident population size of Singapore in 2020 was 4,044,200 citizens and permanent residents, the study suggests that more than 93,000 people had by 2021 consumed illicit drugs at least once in their lifetime – of which 27,000 people (or 28.9%) did so before they turned 18 years old – while 0.7% (28,300 people) had used illicit drugs in the past year. These are not insignificant numbers for a country with a zero-tolerance policy.

Among respondents who reported lifetime illicit drug consumption, cannabis was the most common drug first consumed and the most frequently consumed drug in the lifetime. According to the Alcohol, Drugs and Addictive Behaviours Unit at the World Health Organization, cannabis is the most widely cultivated, trafficked and abused illicit drug globally. About 147 million people, that is, 2.5% of the world population, consume cannabis annually, compared with 0.2% consuming cocaine and 0.2% consuming opiates (World Health Organization, 2016). The short- and long-term consumption of cannabis is associated with several health and social consequences. However, the harm caused by cannabis is often underestimated, which may have contributed to its increased consumption in the past few decades.

Our data also reveals that age, ethnicity, employment status, smoking status and hazardous alcohol use are significantly associated with lifetime illicit drug consumption. The association of drug consumption with the younger age group, smoking and hazardous alcohol use are well-established globally (UNODC, 2021; de Veld et al., 2021). Previous research has found that birth cohort effects are associated with differences in substance consumption, and that these may partially reflect trends in drug popularity, availability and perceptions of reduced harm (Burns et al., 2017; Johnston et al., 2013; Pampel & Aguilar, 2008).

A systematic review of epidemiological studies shows that among adults, current and lifetime smoking is consistently higher among adults with lifetime, past-year and past-month SUDs compared with other adults (Weinberger et al., 2016). While the systematic review could identify fewer studies examining smoking among adolescents with SUDs, the results are similar to those of adult studies. Similarly, data from the 2015 to 2017 National Surveys on Drug Use and Health used to examine past-year SUD comorbidity combinations among 12 substances found that the four most common SUD combinations included alcohol use disorder (Von Gunten & Wu, 2021).

Clinically, assessment and treatment often focus on a substance-specific SUD. However, early diagnosis and intensive treatment of multiple SUDs is of utmost importance. Multiple SUDs are more persistent than individual SUDs and are associated with an elevated risk of developing comorbid psychiatric and physical health problems (McCabe et al., 2017). Furthermore, multiple SUDs may adversely affect treatment outcomes; e.g. cigarette smoking predicts worse treatment outcomes among those with illicit drug dependence (Harrell et al., 2011).

Studies conducted elsewhere have reported an association between unemployment and consumption of illicit drugs (Casal, Rivera, & Currais, 2020; Haddad et al., 2023). Our study, on the other hand, finds that those who are economically inactive or students are less likely to endorse lifetime drug consumption than those who are employed. Several reasons are possible for this association. First, it is possible that given the stringent laws, access to drugs is not easy, and the cost of illicit drugs may be higher in Singapore. These factors may have limited the consumption among the economically inactive and student category who have limited financial resources. Second, it is possible that the economically inactive group, that is, retirees and homemakers, constitutes a low-risk group who are less likely to take drugs. Third, it is also possible that the use of evidence-based approaches in school to prevent substance abuse and other protective factors, such as having a structured curriculum and school connectedness, could have reduced the risk of consumption of illicit substances in students (Griffin & Botvin, 2010; Weatherson et al., 2018). Last, it is possible that those who start consuming drugs at an early age drop out of school (Patrick, Schulenberg, & O'Malley, 2016). This could also lead to the lower association between students and illicit drug consumption observed in the study.

The study also shows that illicit drug consumption is associated with poor health outcomes. Those with lifetime drug consumption are more likely to have clinical anxiety (as assessed by GAD-7), clinical insomnia, self-reported, doctor-diagnosed depression, bipolar disorder, anxiety disorder and psychosis/schizophrenia. While several other studies substantiate these associations, the takeaway point is that the consumption of substances is associated with poor health and well-being of the individual (Compton et al., 2007; Schulte & Hser, 2014; Keaney et al., 2011). However, given this study's cross-sectional nature, we cannot establish causality. While it is possible that substance consumption leads to anxiety, it is also possible that those with anxiety disorders use substances as a form of self-medication (Kushner et al., 2008; Turner et al., 2018).

Certain limitations must be kept in mind while interpreting the results of this study. First, this was a household sample, so it excluded residents of nursing homes, hospitals, prisons and those with unstable housing. Second, about 30% of the sample was not interviewed (due to refusal to participate in the study). This non-response could lead to an underestimation of the true prevalence. Third, participants may have under-reported or denied their symptoms. They might be reluctant to share their personal experiences due to either fear of legal repercussions or embarrassment, as alcohol and drug consumption remain stigmatised behaviours in Singapore. Thus, the true prevalence of drug consumption in Singapore may be higher. Fourth, to ensure confidentiality, we only included respondents who were literate and could complete the questionnaires independently. Fifth, the study results are subjective to recall bias, especially the consumption of substances over a lifetime. Last, this being a cross-sectional study, we cannot determine causality. Thus, the relationship between drug consumption and psychological distress is difficult to establish.

On the other hand, the study has several strengths. First, the study used a nationally representative sample; the response rate of 73% makes our

results generalisable to the Singapore population. The team also put in several safeguards to ensure the confidentiality and protection of personal data, which led to the willingness of people to participate and share information about high-risk behaviours. In addition, stringent quality control measures ensured data integrity and data quality.

In conclusion, this is the first nationwide study that has examined the prevalence of illicit drug consumption in the community-dwelling population of Singapore using robust scientific methods. It is essential to maintain a strong commitment to monitoring relevant changes in the prevalence of drug consumption and the early identification of emerging trends in the attitudes towards the consumption of illicit drugs in the future. Such data will further strengthen preventive and treatment efforts across Singapore.

Funding

The study was funded by the Ministry of Home Affairs and Ministry of Health, Singapore. The funding bodies did not have any role in the data collection, data analysis and writing of this article.

ABOUT THE AUTHORS

Mythily Subramaniam
graduated from the Lady Hardinge Medical College, India. She received her PhD in Gambling Studies from Monash University and is currently Assistant Chairman Medical Board (Research) and Lead Investigator of the Programme of Mental Health Policy Studies at the Institute of Mental Health (IMH). A Consultant with the Singapore Ministry of Health, she also has concurrent teaching appointments as an Associate Professor at the Lee Kong Chian School of Medicine and Saw Swee Hock School of Public Health, National University Singapore. She has worked in the field of mental health for more than 15 years and her main academic and research interests include psychiatric epidemiology, psychosis and addictions.

Koh Yen Sin
is a biostatistician in the Research Division of the Institute of Mental Health. He earned his Master of Public Health (MPH) with a specialisation in epidemiology and quantitative methods from the Saw Swee Hock School of Public Health at the National University of Singapore. His research focuses on mental health outcomes and health behaviours. Koh has contributed to 20 articles in peer-reviewed journals and received the Singapore Young Investigator Award (Health Service Research) – Silver in 2022. Currently, he is examining the prevalence and correlates of smoking-related outcomes using data from the 2022 Health and Lifestyle Survey.

Asharani PV
has been a senior manager for research at the Institute of Mental Health in Singapore since 2015. She holds a PhD from the National University of Singapore and has previously worked as a research fellow at the Institute of Molecular and Cell Biology (A*STAR). Her research spans multiple disciplines, focusing on the epidemiology and neurogenetics of addiction, including tobacco use. She has published multiple articles and systematic reviews on the health implications of substance use. Additionally, Asharani has contributed to understanding the genetic risk factors in substance use through whole-exome sequencing studies and has addressed mental health challenges, such as the use of electronic nicotine delivery systems among individuals with mental illness. She also plays a key role in managing large epidemiological studies, focusing on mental health and diabetes, including the Well-being of the Singapore Elderly (WiSE) study.

Rajeswari Sambasivam
is a manager at the Research Division of the Institute of Mental Health. She has been in the mental health research field for about 13 years and has contributed to articles focusing on mental health outcomes and policy-relevant research. She plays a key role in managing the operational and administrative aspects of population-based studies, ensuring a seamless progress of the projects. She worked on the recent Health and Lifestyle Survey that established the prevalence of consumption of illicit drugs and its correlates in the general population of Singapore. She was presented the Singapore Young Investigator Award (Health Service Research) – Bronze in 2022.

Edimansyah Abdin
is a principal biostatistician at the Research Division, Institute of Mental Health, Singapore. He holds a PhD from Universiti Sains Malaysia. He has been providing statistical support including study design, sample size calculation, performing statistical analyses for nationwide surveys, engaging in several clinical trials, developing a mapping function for cost-utility analyses, and validating the mental health instruments at the Institute of Mental Health since 2009. He was a Principal Investigator for two competitive National Medical Research Council health services research grants to study preference-based measure of health-related quality of life and disability measures and served as a co-Investigator for large psychiatric epidemiology surveys in Singapore.

Janhavi Ajit Vaingankar
is a director at the Research Division, Institute of Mental Health, Singapore. She received her PhD in Public Health from the National University of Singapore. She has over 20 years' research experience that ranges from basic to mental health services research. Her research has focused on psychiatric epidemiology and policy-relevant studies that have addressed real-world challenges faced by individuals with mental disorders and their caregivers. She is a co-investigator on large national studies, including the National Youth Mental Health Study and the Singapore Mental Health Study that have established the prevalence of mental disorders, mental health literacy and barriers to care in Singapore. She leads research on positive mental health at the institute which aims to uncover and measure aspects of mental wellness that are relevant to the local population. She has over 200 publications in scientific journals based on the results arising from her work.

Chua Hong Choon
is the Chief Executive Officer of Khoo Teck Puat Hospital and Yishun Health, and former CEO of the Institute of Mental Health from 2011 to 2021. A psychiatrist by training, he is also Adjunct Professor at the Lee Kong Chian School of Medicine NTU, and Adjunct Associate Professor at Yong Loo Lin Medical School NUS. He completed his undergraduate medical education and post-graduate studies in psychiatry at the National University of Singapore in 1990 and 1996 respectively, and he subsequently held the position of research fellow and visiting faculty at the New York University from 2001 to 2002. In 2012, he completed a Master's degree in Health Care Management at the Harvard School of Public Health. Chua has keen interests in the fields of public health, quality and safety in health care, psychiatric epidemiology, and depression. He completed the first nationwide epidemiological survey of Depressive and Anxiety Disorders in Adult Singaporeans in 2004, and from 2007 to 2010, he was senior consultant of mental health to Singapore's Ministry of Health to oversee several major projects to promote mental wellbeing and to expand mental health services for the nation. Chua also served as chairman of the national Residency Advisory Committee (RAC) for Psychiatry from 2011 to 2021.

Lee Cheng
joined the Institute of Mental Health in 1994. He is currently a psychiatrist and senior consultant as well as the clinical director of the Office of Population Health. Lee is an adjunct associate professor at Lee Kong Chian School of Medicine, Nanyang Technological University and an adjunct assistant professor and clinical senior lecturer at Yong Loo Lin School of Medicine, National University of Singapore. He is also an academic board member for the Executive Counselling & Training Academy and has been a fellow with the Academy of Medicine, Singapore since 2003. He is currently the vice president of the College of Psychiatrists (and a council member since 2017) and serves as the chairman of the Singapore Armed Forces Psychiatry Advisory Board since 2020. Lee is the chair of a Drug Rehabilitation Centre Review Committee since 2021. He is appointed by Ministry of Health to be a council member of the Singapore Medical Council since 2021. Lee is also currently the President of the Singapore Association for Mental Health and a member of the Steering Committee for Beyond The Label 2.0 and the Interagency Taskforce on Mental Health & Well-being.

Chow Wai Leng
is the director of disease policy and strategy at the Ministry of Health, Singapore. She oversees the implementation of policies and disease specific strategies for non-communicable diseases in close collaboration with the Health Promotion Board. This would include upstream preventive health efforts to encourage the population to adopt health lifestyle habits, such as mandatory nutrition labelling of prepacked sugar sweetened beverages and holistically addressing socio-behavioural determinants of health to improve child and maternal health, as well as the disease strategies such as for diabetes. Chow is a family physician by training and has extensive experience in health services research on new care models, implementation research and the application of data analytics and research findings to inform policy and management decision-making in her previous appointments prior to joining the Ministry of Health. She has interests in developing and implementing new care models, as well as the use of research and analytics to enable the adoption of healthy lifestyle behaviours, guide the management of patients and resource allocation. She continues to engage in research and publish on wide range of topics.

Stefan Ma
is currently the deputy director of health analytics at the Ministry of Health, Singapore. His team has been involved in various policy and research projects including national population health surveys, national sero-prevalence surveys, national burden of disease, comparative risk assessments, disease projections, scenario forecast of health policy impacts and interventions on disease burden, disease dynamics modelling, impacts of climate change on health and programme evaluations, which help to support the formulation of national health policies. He is also an adjunct associate professor at the Saw Swee Hock School of Public Health, National University of Singapore and a council member of the Scientific Council for the Global Burden of Disease Study.

Chong Siow Ann
is a senior consultant psychiatrist at the Institute of Mental Health. He has mentored clinicians and researchers in the institute, a few of whom have become either successful researchers or achieved positions of clinical leadership. He was the principal investigator of the first five-year translational clinical research programme in neuroscience (psychosis), and led a group of researchers comprising epidemiologists, biostatisticians and health service researchers who are part of the Programme of Mental Health Policy. He has authored more than 400 journals articles, several in high impact journals that have contributed to a deeper understanding of psychosis, psychopharmacology and stigma towards mental illness. Chong is also on the editorial board of several journals and is on the panel of expert contributors for The Straits Times – his op-ed pieces have led to a deeper understanding and empathy towards those with mental illnesses.

REFERENCES

Ambekar, A., Agrawal, A., Rao, R., et al. (2019). *Magnitude of substance use in India*. New Delhi: Ministry of Social Justice and Empowerment, Government of India.

American Psychiatric Association. (2013). *Diagnostic and statistical manual of mental disorders* (5th ed.). Arlington, VA: American Psychiatric Publishing.

Australian Institute of Health and Welfare. (2020). *National Drug Strategy Household Survey 2019* (Drug Statistic series no. 32, PHE 270). Canberra: AIHW.

Baptiste-Roberts, K., & Hossain, M. (2018). Socio-economic disparities and self-reported substance abuse-related problems. *Addict Health*, 10, 112-122.

Burns, A. R., Hussong, A. M., Solis, J. M., et al. (2017). Examining cohort effects in developmental trajectories of substance use. *International Journal of Behavioral Development*, 41, 621-631.

Casal, B., Rivera, B., & Currais, L. (2020). Economic crisis, unemployment and illegal drug consumption in Spain. *Applied Economic Analysis*, 28, 153-170.

Chong, S. A., Abdin, E., Luo, N., et al. (2012). Prevalence and impact of mental and physical comorbidity in the adult Singapore population. *Annals of the Academy of Medicine, Singapore*, 41, 105-114.

Center for Behavioral Health Statistics and Quality; SAMHSA Administration. (2015). *National Survey on Drug Use and Health: Detailed Tables*. https://www.samhsa.gov/data/report/results-2015-national-survey-drug-use-and-h. Accessed April 7, 2024.

Central Narcotics Bureau. (2023). *News Release*. https://www.cnb.gov.sg/docs/default-source/drug-situation-report-documents/cnb-annual-statistics-2022_final.pdf. Accessed October 2, 2023.

Compton, W. M., Thomas, Y. F., Stinson, F. S., et al. (2007). Prevalence, correlates, disability, and comorbidity of DSM-IV drug abuse and dependence in the United States: Results from the National Epidemiologic Survey on Alcohol and Related Conditions. *Archives of General Psychiatry*, 64, 566-576.

de Veld, L., Wolberink, I. M., van Hoof, J. J., et al. (2021). The role of tobacco smoking and illicit drug use in adolescent acute alcohol intoxication. *BMC Pediatrics*, 21, 233.

European Monitoring Centre for Drugs and Drug Addiction. (2021). *European Drug Report: Trends and Developments*. Luxembourg: Publications Office of the European Union.

European Monitoring Centre for Drugs and Drug Addiction. (2002). *Handbook for surveys on drug use among the general population*. https://www.emcdda.europa.eu/html.cfm/index58052EN.html_en. Accessed April 8, 2024.

Griffin, K. W., & Botvin, G. J. (2010). Evidence-based interventions for preventing substance use disorders in adolescents. Child and Adolescent Psychiatric Clinics of North America, 19, 505-526.

Haddad, R. E., Matta, J., Lemogne, C., et al. (2023). The association between substance use and subsequent employment among students: Prospective findings from the CONSTANCES cohort. *Social Psychiatry and Psychiatric Epidemiology*, 58, 249-266.

Harrell, P. T., Montoya, I. D., Preston, K. L., et al. (2011). Cigarette smoking and short-term addiction treatment outcome. *Drug and Alcohol Dependence*, 115, 161-166.

Johnston, L. D., O'Malley, P. M., Bachman, J. G., et al. (2013). *Monitoring the future national drug use, 1975-2012, Vol 2, College students and adults ages 19-50*. Ann Arbor: Institute for Social Research, The University of Michigan.

Keaney, F., Gossop, M., Dimech, A., et al. (2011). Physical health problems among patients seeking treatment for substance use disorders: A comparison of drug dependent and alcohol dependent patients. *Journal of Substance Use*, 16, 27-37.

Kroenke, K., Spitzer, R. L., & Williams, J. B. W. (2001). The PHQ-9: Validity of a brief depression severity measure. *Journal of General Internal Medicine*, 16, 606-613.

Kushner, M. G., Krueger, R., Frye, B., et al. (2008). Epidemiological perspectives on co-occurring anxiety disorder and substance use disorder. In Stewart, S. H., & Conrod, P. J. (Eds.), *Anxiety and substance use disorders: The vicious cycle of comorbidity* (pp. 3-17). New York: Springer.

McCabe, S. E., West, B. T., Jutkiewicz, E. M., et al. (2017). Multiple DSM-5 substance use disorders: A national study of US adults. *Human Psychopharmacology: Clinical and Experimental*, 32, 10.1002/hup.2625.

Morin, C. M., Belleville, G., Belanger, L., et al. (2011). The Insomnia Severity Index: Psychometric indicators to detect insomnia cases and evaluate treatment response. *Sleep*, 34, 601-608.

Narcotics Division, Security Bureau. (2021). *Central Registry of Drug Abuse Seventieth Report 2012-2021*. Hong Kong Special Administrative Region. https://www.nd.gov.hk/pdf/report/crda_71st/CRDA_71st_Report_Full_Version.pdf. Accessed October 2, 2023.

Pampel, F. C., & Aguilar, J. (2008). Changes in youth smoking, 1976-2002: A time-series analysis. *Youth & Society*, 39, 453-479.

Patrick, M. E., Schulenberg, J. E., & O'Malley, P. M. (2016). High school substance use as a predictor of college attendance, completion, and dropout: A national multi-cohort longitudinal study. *Youth & Society*, 48, 425-447.

Saunders, J. B., Aasland, O. G., Babor, T. F., et al. (1993). Development of the Alcohol Use Disorders Identification Test (AUDIT): WHO Collaborative Project on Early Detection of Persons with Harmful Alcohol Consumption—II. *Addiction*, 88, 791-804.

Schulte, M. T., & Hser, Y.-I. (2014). Substance use and associated health conditions throughout the lifespan. *Public Health Reviews*, 35.

Silins, E., Fergusson, D. M., Patton, G. C., et al. (2015). Adolescent substance use and educational attainment: An integrative data analysis comparing cannabis and alcohol from three Australasian cohorts. *Drug and Alcohol Dependence*, 156, 90-96.

Spitzer, R. L., Kroenke, K., Williams, J. B. W., et al. (2006). A brief measure for assessing generalized anxiety disorder. *Archives of Internal Medicine*, 166, 1092-1097.

Substance Abuse and Mental Health Services Administration. (2020). *Mental health and substance use disorders*. https://www.samhsa.gov/find-help/disorders. Accessed April 8, 2024.

Substance Abuse and Mental Health Services Administration (SAMHSA). (2020). *National Survey of Drug Use and Health (NSDUH) Releases*. https://www.samhsa.gov/data/data-we-collect/nsduh-national-survey-drug-use-and-health. Accessed April 8, 2024.

Substance Abuse and Mental Health Services Administration. (2014). *Results from the 2013 National Survey on Drug Use and Health: Summary of National Findings*. https://www.samhsa.gov/data/report/results-2013-national-survey-drug-use-and-health-summary-national-findings. Accessed April 7, 2024.

Turner, S., Mota, N., Bolton, J., et al. (2018). Self-medication with alcohol or drugs for mood and anxiety disorders: A narrative review of the epidemiological literature. *Depression and Anxiety*, 35, 851-860.

United Nations Office on Drugs and Crime. (2021). *World Drug Report*. www.unodc.org/unodc/en/data-and-analysis/wdr2021.html. Accessed April 8, 2024.

Von Gunten, C. D., & Wu, L. T. (2021). Comorbid substance use disorder profiles and receipt of substance use disorder treatment services: A national study. *Journal of Studies on Alcohol and Drugs*, 82, 246-256.

Weatherson, K. A., O'Neill, M., Lau, E. Y., et al. (2018). The protective effects of school connectedness on substance use and physical activity. *Journal of Adolescent Health*, 63, 724-731.

Weinberger, A. H., Funk, A. P., et al. (2016). A review of epidemiologic research on smoking behavior among persons with alcohol and illicit substance use disorders. *Preventive Medicine*, 92, 148-159.

World Health Organization. (2016). *The health and social effects of non-medical cannabis use*. https://www.who.int/teams/mental-health-and-substance-use/alcohol-drugs-and-addictive-behaviours/drugs-psychoactive/cannabis. Accessed October 3, 2023.

SAFETY MORE THAN DETERRENCE
A COMMENTARY ON CAPITAL PUNISHMENT

Euston Quah & Tan Jun Rui
Economic Growth Centre, Nanyang Technological University, Singapore

ABSTRACT

Recent polls conducted or commissioned by the Ministry of Home Affairs (MHA) reveal that a majority of surveyed Singaporeans and regional residents support capital punishment, with many believing it effectively deters drug trafficking and other serious crimes. Beyond its deterrence effect, we argue for an equally important intangible benefit: the safety assurance effect. While deterrence focuses on crime prevention, it may not always align with the public's sense of safety. However, these feelings of safety contribute to broader societal benefits, such as increased productivity, enhanced well-being, and strengthened public trust in the government's role in safeguarding society. By integrating both the deterrence and safety assurance effects, policymakers can develop a more comprehensive framework for assessing the legitimacy and efficacy of capital punishment.

Several months ago, a 45-year-old man in Singapore was arrested for suspected drug trafficking. Authorities seized an alarming quantity of heroin – nearly 180 times the minimum amount that warrants the death penalty upon conviction.[1] Besides alluding to the effectiveness of Singapore's law enforcement in nabbing the trafficker, this incident drew attention once again to whether capital punishment is effective in deterring crime.[2]

Recent polls conducted or commissioned by the Ministry of Home Affairs (MHA) show that most surveyed Singaporeans are very much in support of the death penalty as an appropriate punishment for drug trafficking and other serious crimes, with deterrence being a strong justification, while most surveyed residents in the region perceive it as a more effective deterrent than life imprisonment in Singapore (MHA Research and Statistics Division, 2021; MHA Home Team Behavioural Sciences Centre, 2018).

However, some may argue that the perceptions of victims and society-at-large towards the deterrence effect of capital punishment carry less weight, as the concept of deterrence ultimately hinges on whether potential perpetrators are actually deterred or not.

Even if scientific studies could establish a clear deterrence effect, it simply means that, on average, the deterrence effect is present but not guaranteed in every instance. This is crucial because Singapore cannot afford the risk that even a few individuals who might have been deterred from drug trafficking become undeterred due to the easing of capital punishment. As a small and densely populated state, Singapore could experience faster and more noticeable negative effects to society if drug distribution increases even slightly.

[1] Under Singapore's Misuse of Drugs Act, a person found guilty of trafficking more than 15g of heroin faces a mandatory death penalty. In announcing the arrest of a 45-year-old man for suspected drug trafficking in April 2024, the Central Narcotics Bureau stated that 2,682g of heroin, 20g of Ecstasy, 10g of Ice (methamphetamine), 10g of cannabis and two Erimin-5 tablets were seized from his person and a hideout he was using (Sim, 2024).

[2] Under Singapore law, crimes punishable by death include murder, terrorism, drug trafficking, use of firearms and kidnapping. The majority of capital offences are, however, for drug trafficking, the other crimes being relatively rare in Singapore.

Moreover, addressing the consequences of widespread drug issues can be as challenging and costly as restoring damaged natural ecosystems, often more so than preventing them in the first place. The total cost of drug crime in Singapore in 2015 was estimated at S$1.23 billion (Quah et al., 2025 [Forthcoming]; Wong, 2020). This figure is likely to be an underestimation considering that it excludes productivity losses due to illness and productivity losses incurred by caretakers of drug abusers[3] (Koh, 2020).

Focusing solely on deterrence overlooks the broader issue of improving societal welfare –namely, what it takes to make people feel safe and secure. Instead of focusing only on how crime reductions are achieved, we should not only understand but also measure society's attitudes and tolerance towards maintaining a crime-free environment.

We argue that there is potential for the value of public safety to complement the deterrence effect of capital punishment in making a stronger case for Singapore's legal stance towards serious crimes in society.

Safety assurance ≠ crime deterrence

The terms "deterrence" and "safety" are often used interchangeably in the context of capital punishment. While it is true that maintaining public safety is an outcome of effective deterrence, there are some differences between the two because deterrence focuses more on the perpetrator, while safety is more centered on the victim.

Even if crime rates are low, this does not necessarily mean that people feel safe and assured of their safety. For instance, low crime rates might also result from underreporting of crimes or a lower propensity for crime due to an aging population, rather than merely reflecting the quality of local law enforcement. People's perceptions of safety can be influenced by individual experiences, media reports, and community stories of high-profile crimes, which can inflate the sense of danger and undermine feelings of safety regardless of actual crime rates. This paradoxical relationship between actual crime rates and perceptions of safety was also highlighted in a 2013 article from The Guardian based on the United Kingdom context (Bonnet, 2013).

Public safety has broader implications for society which would not be captured if it is anchored to the deterrence effect of capital punishment. The assurance effect of public safety in reducing the risk of harm or injury produces less anxiety among the community, enhances well-being and hence leads to higher work productivity. It also promotes a sense of governmental accountability in protecting society from crime, while also fostering trust and confidence in other legislative measures and policies.

In the poll conducted by MHA, maintaining safety in Singapore through deterrence or incapacitation was among the least-cited reasons for supporting capital punishment. However, when the safety reason was framed in terms of the danger it poses to society, it was the top-cited reason for supporting capital punishment for drug trafficking and firearm offences (MHA Research and Statistics Division, 2021). In the other poll commissioned by MHA that assessed the perception of safety in general terms rather than specifically in the context of deterrence, most respondents indicated that they feel safe and assured of their safety from crime while travelling in Singapore (MHA Home Team Behavioural Sciences Centre, 2018). This illustrates the importance of distinguishing between the safety assurance effect and the crime deterrence effect, and the need to clearly define the former.

Studies needed

Just like environmental and heritage goods, deterrence and public safety can also be perceived as nonmarket goods that are produced by capital punishment, meaning they do not have a direct market price.

As with most commodities, provision of safety involves the utilisation of resources which have competing uses. Measuring both the tangible and intangible benefits of being safe and feeling safe may help the government to determine the optimal allocation of resources for criminal justice

[3] Also see Quah et al. (2020) for a review of general methodologies used to estimate the tangible and intangible costs of drug crime.

expenditures. Understanding the monetary value of safety is an important first step for the government to minimise the risk of over- or under-spending on policing measures to detect and prevent criminal offenses that warrant capital punishment.

Assuming that crime prevention strategies, including capital punishment, entail costs to taxpayers, the public could be surveyed about their willingness to pay for these strategies if they are assured of recent reductions in crime rates. This willingness to pay reflects the public's desire for safety, rather than serving as an objective measure of crime deterrence (Cohen et al., 2001).

By gathering information on how an improvement in public safety benefits their everyday lives such as commuting to work and travelling outdoors comfortably, as well as maintaining healthy relationships with friends and family members, we can better understand the value of safety that people are willing to pay for.

In addition to improving quality of life, the benefits of increased safety assurance can be compared across different jurisdictions with varying legal systems. For instance, one could examine how much workplace absenteeism is related to fear of going outdoors in countries with less stringent policies relative to capital punishment on drug trafficking, firearms, and intentional murder.

Bottom line

Most would agree that it is better to draft capital punishment laws around the assumption that death penalty deters crime even if it actually does not, rather than to assume that it does not deter crime when it actually does. Any margin of error associated with the latter can have devastating consequences for Singapore.

Capital punishment laws affect not only the perception of deterrence but also safety. The broad concept of safety is often mentioned in tandem with, and thus partially obfuscated in arguments for deterrence. However, assurance of public safety may, in its own right, also be meaningful in enriching the discourse of capital punishment and crime prevention policies in general. Demands for safety by society itself justify public action and reveal how public perception on capital punishment brings assurance on safety. This is more than enough reason beyond deterrence.

ABOUT THE AUTHORS

Euston Quah
is Albert Winsemius Chair Professor of Economics, and Director of the Economic Growth Centre at Nanyang Technological University. Professor Quah has published over 100 articles in journals and lead opinion pieces in the media. He is the author of the bestselling Asian edition of Gregory Mankiw's leading textbook, *Principles of Economics*, and the internationally known book, *Cost-Benefit Analysis*. He also wears multiple hats as Editor of the *Singapore Economic Review*, President of the Economic Society of Singapore, and member of the prestigious European Academy of Sciences and Arts.

Jun Rui Tan
is a researcher in the Economic Growth Centre at Nanyang Technological University, with a bachelor's degree in economics. Since 2022, he has been working with his mentor Professor Euston Quah on publishing opinion articles in local media on potential topics where cost-benefit analysis can be applied. Research areas of interest include sustainability development goals, valuation of intangible goods and social welfare.

REFERENCES

Bonnet, M. (2013). Even though crime levels are falling, why don't we feel safer? *The Guardian*.

Cohen, M. A., Rust, R. T., Steen, S. & Tidd, S. T. (2001). *Willingness-to-Pay for Crime Control Programs*. Retrieved from: https://ssrn.com/abstract=293153 or http://dx.doi.org/10.2139/ssrn.293153

Koh, F. (2020). Parliament: $1.23 billion cost to Singapore of drug crimes 'an underestimation', says Sun Xueling. *The Straits Times*. Retrieved from https://www.straitstimes.com/singapore/parliament-1-23-billion-cost-to-singapore-of-drug-crimes-an-underestimation-sun-xueling

Ministry of Home Affairs (MHA) Home Team Behavioural Sciences Centre (2018). Perception of Residents in Regional Cities on Singapore's Crime Situation, Law and Safety. Retrieved from https://www.mha.gov.sg/mediaroom/press-releases/findings-from-recent-studies-on-the-death-penalty-in-singapore/

MHA Research and Statistics Division (2021). Survey on Singapore Residents' Attitudes towards the Death Penalty. Retrieved from https://www.mha.gov.sg/mediaroom/press-releases/findings-from-recent-studies-on-the-death-penalty-in-singapore/

Quah, E., Chia, W. M., & Tan, T. S. (2020, January). Costs of Drug Crime: Literature Review and Methodology. *Home Team Journal Special Issue: Spotlight on Drugs*.

Quah, E., Chia, W. M. & Tan, T. S. (Forthcoming 2025). Cost of Drug Crime in Singapore. *The Singapore Economic Review*, Special Issue of The Singapore Economic Review — "In Memoriam Professor Jack L. Knetsch on Environmental Economics and Cost-Benefit Analysis", vol. 2.

Sim, S. (2024, 18 April). Man arrested, $286k worth of cannabis, Ice, heroin and other drugs seized: CNB. *The Straits Times*. Retrieved from https://www.straitstimes.com/singapore/courts-crime/man-arrested-286k-worth-of-cannabis-ice-heroin-and-other-drugs-seized-cnb

Wong, C. (2020, January 21). Drug crimes cost Singapore $1.23 billion in 2015, NTU study finds. *The Straits Times*. Retrieved from https://www.straitstimes.com/singapore/courts-crime/drug-crimes-cost-singapore-123-billion-in-2015-ntu-study-finds

THE DEADLY NARRATIVES OF TERRORIST FINANCING IN INDONESIA

Noor Huda Ismail
S. Rajaratnam School of International Studies, Singapore

ABSTRACT

Terrorist networks use narratives for various purposes, spanning recruitment to fundraising. Some of these narratives have been very effective in coaxing ordinary individuals to contribute their money through evocative slogans such as "Donations should come from the heart" and "Do you desire paradise? Let's donate." These are spiritually appealing to Indonesians, especially Muslims. In examining the issue of terrorist funding in Indonesia, this article focusses on narratives crafted by two terrorist groups, Jemaah Islamiyah and Jemaah Ansharut Daulah, to rally support for their cause. By deconstructing these narratives and their appeal to different vulnerable communities, including female migrant workers, the article also addresses the question of why people desire and express interest in financially supporting terrorism. Recommendations are offered on counter narrative strategies to disrupt and undermine the ability of extremist groups to garner public support.

TERRORIST NARRATIVES IN ACTION

Solo, Central Java, Indonesia, March 10, 2022.

As sympathisers and family members gathered in the heavy rain to pay their final respects to Sunardi, a prominent figure within Jemaah Islamiyah (JI), Ustad Abdurrahman, a religious leader, led the final prayers. "Paralyze the hands of the oppressors. ... destroy them … leave them not in this world. ... [for] they have harmed your guardians," his anguished cries pierced the air. He ended the vigil with this impassioned plea:

> *O Allah, don't let us be humiliated like this ... O Allah, raise the banner of Islam, win over your guardians, O Allah. ... Make his blood a light for the believers and hell for the wrongdoers. ... O Allah, let his martyrdom guide his family in Your mercy....*

The invocation of divine intervention to paralyse oppressors and seek retribution are recurring themes within extremist narratives. Funeral prayers after the death of a group member are carefully crafted to not only cope with the loss but to also reinforce the collective identity, the group's resilience and its commitment to the ideological cause. In the face of adversity, the community is reminded to unite under the banner of Islam, seeking strength and divine intervention to overcome perceived injustices.

Abdurrahman, in invoking this narrative of martyrdom, turned the death of a leader of the JI terrorist group killed in a police raid, into a symbolic act of resistance against perceived oppression. His prayers served two purposes – to inspire and strengthen internal cohesion, while portraying external adversaries as recipients of divine retribution. The narrative positioned the dead man's life within an overarching and comprehensive storyline that extended beyond individual events, offering a cohesive and impactful account of his group's activities, objectives, and worldview.

This article discusses the faith-based narratives constructed by the terrorist groups Jemaah Islamiyah (JI) and Jemaah Ansharut Daulah (JAD) to rally the public to their cause, especially by supporting terrorist financing in Indonesia. These narratives are strategically wielded, especially at funerals of their members to foster a sense of distrust or animosity towards government actions in the eyes of the wider community. The narratives are thus key to understanding how ordinary people

become supporters of terrorist organisations. Powerful narratives can replace an individual's common sense with a new way of looking at the world, justifying violent actions and mobilising financial support.

WHAT ARE NARRATIVES?

Narratives, as explained by scholars like Ajit K. Maan and Paul L. Cobaugh in their seminal work *Introduction to Narrative Warfare* (2022), are distinct from mere stories. While stories are only retellings of the who, what, where, when, why, and how of a past event, narratives serve a more strategic function. Narratives provide interpretation, framing, or meaning of past events, usually moving the audience towards a particular course of action or mindset. The distinctive feature of a narrative lies in its interpretative nature, making it far from a neutral or value-free process.

Narratives can take the form of speech or visual media. Spoken narratives – in the form of lectures, discussions, book reviews, stories, or prayer testimonies – are often disseminated through various channels such as the sermons of charismatic leaders on online platforms. These narratives may glorify acts of violence, present a distorted version of historical events, or propagate a utopian vision of a society governed by a particular ideology. Speeches are particularly useful for systematically appealing to identity, articulating the tenets of an ideology, and creating a sense of urgency. Through carefully chosen words, intonations and gestures, a skilled orator can stir feelings of anger, righteousness, fear or hope in their audience.

Visual narratives, on the other hand, leverage images, videos, and symbols to reinforce and amplify the ideological messages. Visual media – encompassing writings, posters, pamphlets, pictures, and videos – transcend the limitations of language and harness the evocative potential of symbolism. Every image, every video clip is laden with layers of meaning, tapping into the subconscious minds of viewers to evoke visceral and emotional responses. From slickly produced videos extolling the virtues of a particular ideology to compelling posters evoking feelings of pride and solidarity, these propaganda materials serve as potent tools for ideological indoctrination.

In the digital age, social media has emerged as a battleground for the dissemination of visual narratives. Platforms like Facebook, X (formerly known as Twitter) and Instagram are awash with images, videos, and memes designed to propagate specific ideologies and worldviews. These visual representations, shared and reshared countless times, have the power to reach millions of individuals within seconds, amplifying the reach and impact of the underlying narrative. In effect, visual narratives provide a sense of coherence and continuity to the ideological landscape. Crucially, visual narratives play a pivotal role in fostering a sense of belonging and identity within a larger cause.

The power of narratives, whether conveyed through spoken words or visual representations, is considerable as they shape not only **individual perspectives** but also **collective perceptions**. By presenting a compelling vision of a shared destiny, they create a collective consciousness among individuals susceptible to radicalisation, forging bonds of solidarity and camaraderie that transcend individual differences. This effect of fostering collective consciousness is particularly pronounced in the context of **grand narratives**.

GRAND NARRATIVES: A COMMON TRUTH

While a narrative typically caters to a single event, grand narratives – also known as master narratives – are comprehensive and sweeping ideological frameworks that provide interpretations of events over an extended period. Whether through religious doctrines, political ideologies, or cultural movements, grand narratives provide a sense of meaning, purpose, coherence, and belonging to adherents.

Grand narratives are often visible in a country's national ethos. An example is the American Dream, pervasive in the United States, embodying the belief in universal success through hard work. Southeast Asia, with its diverse tapestry, holds grand narratives crucial to its identity. Indonesia's *Pancasila*, the five foundational principles of the nation-state, is a unifying force that shapes the nation's identity, fostering inclusivity. Malaysia's *Bangsa* Malaysia envisions a collective identity beyond ethnic differences, while Vietnam's narrative of reunification emphasises resilience against foreign intervention. In the Philippines, the People Power Revolution symbolises democratic resilience,

showcasing the ability to overcome political repression. These examples underscore the pivotal role grand narratives play in nation-building, shaping collective memory and contributing to the socio-political fabric of Southeast Asia.

Within the Islamic context, grand narratives often derive from Qur'anic stories, hadiths, or the historical accounts of Islamic struggles, such as the Battle of Badr, the hijra (Prophet Muhammad's migration from Mecca to Medina), and the pre-"Western" colonial Islamic caliphate. These narratives carry immense weight, serving as the cultural bedrock that shapes collective beliefs and values. They resonate deeply within the community, embodying shared experiences and providing a framework for understanding the world. For example, the story of the Battle of Badr, a pivotal event in early Islamic history, is a grand narrative illustrating divine support for the believers in their struggle against oppression.

JI'S GRAND NARRATIVE: "DEFENDER OF THE OPPRESSED"

Abdurrahman's prayers at Sunardi's death vigil reveals the intricacies of the grand narrative of martyrdom cultivated by JI, where the death of a member becomes a guiding light for believers and a source of divine punishment for wrongdoers. In the JI universe, rituals and prayers are not only spiritual, they are strategic. By intertwining the JI narrative with the religious fervour of a funeral, JI aims to shape the emotional responses, perspectives, and collective identity of the community.

As a tool of ideological construction, JI's grand narrative carefully weaves together historical grievances, religious principles, and a call to arms. By presenting their narrative in a grand and all-encompassing manner, JI seeks to establish a framework through which individuals can interpret the complexities of their activities. This overarching storyline creates a sense of coherence and purpose, fostering a collective identity among supporters and sympathisers.

JI's grand narrative positions it as a defender of the oppressed. This narrative serves a dual purpose of shaping the collective identity of its members while casting doubt on the credibility of counter-terrorism efforts by state security forces. The carefully crafted narrative blurs the line between right and wrong, presenting JI as a righteous force combatting perceived oppression.

Sunardi's death during a Detachment 88 operation on 9 March 2022 gave JI such an opportunity. Detachment 88 had urged Sunardi to surrender peacefully. However, Sunardi resisted, resulting in a violent confrontation that led to his demise.

A war of narratives followed. While the government narrated the fatal operation as a win against terrorism, JI portrayed it as a clash of ideologies, framing Sunardi's resistance as a valiant stand against perceived oppression. By emphasising the use of force by Detachment 88, JI sought to depict the government as an aggressor, thereby reinforcing their narrative of resistance and framing their struggle as a righteous cause. This portrayal aligns with broader narratives propagated by extremist groups, where confrontations with security forces are presented as acts of martyrdom and resistance in the face of perceived tyranny.

The strategic manipulation of this event within JI's group narrative serves multiple purposes. Firstly, it strengthens the ideological cohesion within JI, rallying members around a shared sense of victimhood and resistance against state authorities. Secondly, it reinforces the narrative of a broader societal struggle against external forces, appealing to sympathisers and potential recruits who may resonate with the perceived injustice portrayed in the narrative. Lastly, it contributes to shaping public perceptions, fostering a sense of distrust of the government.

Jemaah Islamiyah's grand narrative positions it as a defender of the oppressed. This narrative serves a dual purpose of shaping the collective identity of its members while casting doubt on the credibility of counter-terrorism efforts by state security forces, blurring the line between right and wrong, and presenting JI as a righteous force combatting perceived oppression.

In this way, the confrontation between Detachment 88 and Sunardi serves as a pivotal moment within the group narrative woven by JI, illustrating the strategic intertwining of real-world events with ideological constructs. Understanding the significance of such events in the narrative landscape is essential to deciphering the motivations, actions, and resilience of extremist groups in their pursuit of ideological objectives.

Waging Narrative Warfare

For terrorist groups, the battleground transcends the physical realm, extending into the emotional domain of narrative warfare. Unlike conventional warfare with its territorial pursuits, extremist groups engage in a simultaneous defence and attack through **narrative manipulation**, aiming for the profound moulding of individuals' thoughts and consciousness.

Narrative warfare is a calculated and systematic effort by terrorists to counter prevailing opinions in mass media, whether on television, newspapers, or reputable online sources, that condemn their violent acts. It is crucial to note that those arrested for terrorism often hold respected positions in society—religious preachers, doctors, or even civil servants. The strategic leverage of their positive community image becomes a potent asset in the war of narratives, sparking a clash between the narratives propagated by terrorists and those condemning their actions. This intricate interplay underscores the complex dynamics of narrative warfare, misinformation, and conspiracy theory that unfolds between supporters of terrorism and security forces.

Crucially, the emphasis on narratives employed by terrorist groups is not an academic abstraction; it is firmly rooted in the real life implications of their narrative strategy, repercussions that echo with death and destruction. In the aftermath of harrowing events like bomb explosions or arrests of terrorists, a war of narratives inevitably follows. By dissecting how these groups wield narratives, we may be able to uncover the profound impact of their strategies on individuals and society at large.

GROUP NARRATIVES: THE ART OF REFRAMING HISTORY

Group narratives refer to shared stories, beliefs, and interpretations of events that are collectively constructed and maintained within a social group or community. These narratives play a crucial role in shaping group identity, cohesion, and behaviour, as they provide members with a sense of belonging and common purpose.

Group narratives justify group actions or strategies by linking them to a grand narrative. They do this by strategically connecting widely accepted grand narratives to contemporary issues using a technique known as **reframing**. It is a technique in narrative study that involves *shifting or changing the way a story is presented or interpreted*. It involves looking at a narrative from a different perspective, altering its context, or emphasising different elements to provide new meanings or insights.

Unlike complex scientific methodologies, reframing relies on analogies and metaphors to elicit emotions and captivate the audience. A notable example of this technique is found in the narrative of the Pharaoh in the Qur'an, where historical events are creatively reframed to convey specific messages without relying on intricate scientific approaches. The metaphorical use of Pharaoh in the Qur'an often serves to symbolise an oppressive and dictatorial ruler. This symbolic representation becomes a potent reframing tool, enabling narrators to draw parallels between historical figures and present-day leaders, shaping the audience's perception through emotionally charged analogies.

An illustrative case of this reframing technique was witnessed in the aftermath of Egyptian President Anwar Sadat's assassination during a military parade in 1981. Khalid al-Islambouli, the assailant, used the metaphorical language of the Qur'an, exclaiming, "I have killed Pharaoh" after the assassination. This powerful statement strategically reframed the act, transforming it from a political event into a symbolic confrontation against tyranny, resonating with the Quranic broader narrative of standing up against oppressive rulers. The technique of reframing,

using analogies and metaphors, thus becomes a compelling tool in evoking emotions and shaping perceptions, offering a narrative that transcends the complexities of scientific methodologies while profoundly impacting the audience's imagination and emotions.

INDIVIDUAL NARRATIVES: THE RADICALISING MOTIFS

In the context of terrorism, narratives serve as a key determinant in the radicalisation of individuals within susceptible communities. For a person to be radicalised, groups must be able to significantly influence individual narratives. Individual narratives refer to the personal stories, experiences and perspectives of individuals. These narratives are unique to each person and often shape their identity, beliefs and worldview. Individual narratives can encompass various aspects of a person's life, including their upbringing, cultural background, personal achievements, struggles and relationships.

However, it is essential to recognise that individual narratives are subjective and may not represent the experiences of everyone affected by a particular issue. Moreover, individual narratives can be influenced by factors such as bias, perspective and personal interpretation, highlighting the importance of considering multiple viewpoints when considering complex issues. To truly understand the intricate process of radicalisation, it becomes imperative to examine the interpretative lens through which narrators convey their messages.

Narratives in the realm of radicalisation serve as more than mere storytelling; they act as ideological frameworks that shape individuals' worldviews and influence their belief systems. The storytellers, or narrators, strategically craft and disseminate these narratives, targeting vulnerable individuals who may be seeking meaning, purpose or identity, by presenting a skewed interpretation of events to fit a radical ideology. In essence, narratives in radicalisation act as a powerful force that shapes perceptions, influences attitudes and guides behaviour.

To understand why terrorist organisations choose a particular narrative, we need to understand the underlying motives, emotional triggers and psychological tactics involved. The framing of narratives often exploits grievances and psychological vulnerabilities, capitalising on feelings of marginalisation, injustice or perceived threats in situations of socio-political tension. By understanding how these narratives resonate with the experiences and emotions of the target audience, it becomes possible to unravel the mechanisms through which radicalisation takes root.

Deciphering the interpretative lens provides insights into the manipulative techniques used by narrators to draw individuals into the fold of radical ideologies. By scrutinising the narratives' origins, and methods of dissemination, it becomes possible to develop more targeted and effective counter-radicalisation strategies that address the root causes and mechanisms driving the process of radicalisation.

Researchers investigating the actions of radical movements have identified a diverse array of narratives employed by such groups. These narratives encompass concepts such as *al-walā' wa al-barā'* (the imperative to congregate with like-minded individuals and distance oneself from those with differing ideologies), the struggle of the ummah to restore Islam's former glory, and distorted interpretations of Western movements perceived as detrimental to Muslim families, including family planning, human rights, gender equality, and issues related to the LGBTQ+ community.

An additional narrative revolves around the purported obligation to protect wives and families from slander, attributed to societal systems controlled by thoghut[1] (oppressive) governments that permit women to work outside the home or remain uncovered. These multifaceted narratives present a dual-edged coin that, when combined, poses a new and potent threat. While there is extensive research about terrorism and its connection to religious interpretative narratives, the exploration of funding-related aspects remains notably limited.

[1] In Arabic, "thoghut" طاغوت refers to a tyrant, oppressor, or unjust ruler who deviates from the path of righteousness and justice. It is often used in Islamic literature to denote leaders or systems that promote falsehood, oppression, or disobedience to God's commands. These leaders are seen as usurping divine authority and leading people away from the true path.

EXPLOITATION OF GRAND NARRATIVES FOR TERRORIST FINANCING

This article employs the definition of terrorist financing used in Indonesia's Anti-Terrorism Financing Law No. 9 of 2013: "Every direct or indirect action in supporting, collecting, giving, or lending with the intent to fund terrorist activities, terrorist organisations, or terrorist individual."

Since extremist groups use grand narratives as a lens through which individuals and groups perceive their place in the world, the financing of terrorism becomes intertwined with these narratives as individuals and networks contribute funds to support what they perceive as a righteous cause. The narrative of a perceived clash of civilisations, for instance, fosters a sense of urgency, motivating individuals to contribute financially to groups that claim to defend their cultural or religious identity against perceived external threats.

The financing of terrorism is not merely a financial transaction; it is a manifestation of individuals aligning their resources with a larger narrative that they believe in. The funds contributed are seen as investments in a broader struggle, reinforcing the ideological foundation that justifies the actions of extremist groups.

JI and the pro-ISIS JAD have had a long runway to hone sophisticated approaches that combine emotional appeal, grand narratives, and organisational subterfuge to achieve their financial and operational goals.

Over the years, JI and JAD have deftly reframed and exploited established grand narratives, intertwining their objectives with deeply ingrained cultural and religious beliefs. This manipulation has allowed them to cloak their actions in righteousness, influencing public perception and garnering financial support for their clandestine agendas.

For instance, they have strategically reframed the narrative of Abdur-Rahman Bin Auf, a generous companion of Prophet Muhammad, to establish a seemingly charitable organisation named after him. Abdur-Rahman's authentic narrative embodies generosity and brotherhood. In challenging circumstances, he declined Sa'd Bin Al-Rabi's generous offer, choosing instead to work hard and contribute to the community. Over time, he became prosperous but remained committed to acts of kindness, inspiring generations.

JI exploits this narrative by establishing the Lembaga Amil Zakat Abdur-Rahman Bin Auf (LAZ-ABA), a purported non-profit organisation. They strategically place charity boxes across Indonesia, exploiting emotionally charged religious narratives. This seemingly charitable front conceals a sinister purpose – the financing of terrorism, including weapons procurement. The grand narrative of aiding the oppressed serves as a smokescreen for their illicit activities, exploiting the innate generosity of the Indonesian population.

To further propagate its deception, JI established the Hilal Ahmar Society Indonesia (HASI) in 2008, registering it as a non-profit organisation. Operating under the guise of a social, health, and humanitarian entity, HASI provided JI with a cloak of legitimacy, allowing it to gain public trust. This trust, once established, became a vehicle for the dissemination of JI's ideology and propaganda. When civil war erupted in Syria, HASI's purported humanitarian missions also provided JI with an operational cover to conceal its dispatch of combatants to Syria.

The emergence of HASI can be attributed to the lack of stringent regulations governing non-profit fundraising mechanisms in Indonesia. Until it was designated by the United Nations for terrorist recruitment and funding in 2015, HASI's freedom to collect funds for humanitarian missions to Syria illustrated the challenge of monitoring and deterring fund raising by extremist groups.

The groups have also been able to evolve their tactics. To finance a chilling plot targeting the Indonesian Presidential Palace in December 2016, the JAD in Central Java established a charity organisation as a religious initiative for da'wah (missionary work), concurrently using it to raise funds for their terrorist acts. Unlike JI, JAD extensively leverages social media for fundraising, showcasing how their narratives can be adapted for new platforms. The Facebook posts by Aseer Cruee Center, a terrorist fundraising organisation disguised as a charity, illustrate the impact of narrative manipulation, seamlessly blending religious quotes, financial updates, and calls for support.

Furthermore, JAD's narrative extends beyond fundraising, concealing its primary aim with activities such as education. Its GASHIBU (Gerakan Sehari Seribu, meaning "The one thousand rupiah a day movement") programme directs part of the community donations towards educating the children of terrorist supporters. This not only diversifies their sources of support but also legitimises their activities in their strongholds across West Java, Central Java, and Central Sulawesi.

In this regard, it is critical to acknowledge that terrorist groups like JI and JAD did not emerge in isolation but rather as reactive entities to systemic shortcomings within the state. These deficiencies, spanning from insufficient access to education and healthcare to a dearth of social welfare provisions, sow the seeds of discontent and disenchantment among marginalised communities. It is within this environment of frustration and disillusionment that extremist groups find fertile ground to propagate their ideologies, recruit adherents, and generate funding.

Grand narratives act as a lens through which individuals and groups perceive their place in the world, shaping their motivations and guiding their actions. The financing of terrorism becomes intertwined with these grand narratives as individuals and networks contribute funds to support what they perceive as a righteous cause. The narrative of a perceived clash of civilisations, for instance, fosters a sense of urgency, motivating individuals to contribute financially to groups that claim to defend their cultural or religious identity against perceived external threats.

The financing of terrorism is not merely a financial transaction; it is a manifestation of individuals aligning their resources with a larger narrative that they believe in.

Sidney Tarrow, in his *Power in Movements: Social Movements and Contentious Politics* (1998) posits that political movements often arise as oppositional responses to discontent in society, for example due to issues like poverty, social inequality, corruption, despotism and limited avenues for meaningful political participation.

In Indonesia, terrorist groups like JI and JAD capitalise on this discontent by framing themselves as agents of change and resistance against perceived injustices perpetrated by the state and mainstream political institutions. By aligning their ideologies with the grievances of marginalised communities, these extremist organisations effectively consolidate support, recruit followers, and generate financial resources. They exploit the frustrations and disillusionment of individuals who feel marginalised or excluded from the political process, offering them a sense of purpose, identity and belonging. Moreover, the absence of viable alternatives or effective channels for addressing grievances further exacerbates the appeal of extremist narratives.

In the absence of an effective counter-narrative, these interpretations gain traction, shaping perceptions about the obligation to engage in jihad, as highlighted by the testimonies of captured terrorists.

GENDER IN TERRORIST FINANCING NARRATIVES

The grand narratives crafted by JI and JAD extend their profound influence through a carefully segmented approach, strategically targeting different demographics within society. Particularly significant is the gendered narrative that underscores the varied ways in which these groups tailor their messages to appeal to and involve both men and women in their ideological framework.

The gendered narrative reflects the understanding that societal roles and expectations differ based on gender. By recognising and exploiting these differences, extremist groups aim to broaden their influence and support base. This approach allows for the construction of a more inclusive narrative that appeals to a diverse audience and addresses various societal dynamics.

For male recruits, the grand narrative often emphasises notions of masculinity, heroism, and duty. The overarching story may depict participation

in extremist activities as a means for men to fulfil their roles as protectors and defenders of their communities, religions, or against perceived injustices. Central to this narrative are appeals to a sense of honour, bravery, and a duty to safeguard one's cultural or religious identity, aligning with specific societal expectations of masculinity.

Simultaneously, the grand narrative tailored for youths is centred around the concept of *hūrun'ain*, commonly translated as the "beautiful-eyed angel". This narrative derives from verse 22 of Surah Al-Waqi'ah in the Quran and is intricately framed to convey God's promise to courageous young individuals prepared to sacrifice their lives for jihad. This narrative thread is crafted to be compelling, seeking to draw in and mobilise youths within their ranks. The concept of *hūrun'ain* becomes a powerful element in the narrative, serving as a motivational force to inspire and galvanise the younger demographic toward extremist activities.

On the other hand, the narrative for women is often crafted to align with traditional roles of caregivers, mothers and supporters. Extremist groups may frame their activities as a means for women to contribute to the preservation of their cultural or religious heritage, often emphasising the importance of raising children with the "correct" values. This narrative can be compelling, as it taps into deeply ingrained cultural norms and expectations surrounding women's roles in society.

Other narratives targeted at women include "going to heaven as a family", drawing inspiration from Surah Al-Mu'min verse 8. This narrative gained tragic prominence after the 2018 family suicide bombing incidents in Surabaya. A family of six attacked three churches on 13 May 2018, and another family of five detonated explosives at the entrance of the Surabaya police headquarters the next day. These attacks were the first perpetrated by families, including women and children, in Indonesia and serve as a heartrending reminder of the insidious nature of extremist narratives, particularly their ability to exploit vulnerable individuals and manipulate cherished values for nefarious ends. In this narrative, women are not merely passive participants but active agents recruited to perpetrate violence in the name of a distorted interpretation of religious doctrine.

The narratives for women often emphasise the virtues of revered figures such as Fatimah, the Prophet's daughter, or the story of Ummu Mutiah. Ummu Mutiah, depicted in a hadith as the first woman destined for heaven due to her steadfast protection from fitnah – from moral and spiritual temptations, from being led away from the path of righteousness – because she avoided all interactions with men not considered her muhrim (family member or guardian), serves as an inspirational narrative. The depiction of Fatimah's admiration for Umm Mutiah, known for her neat appearance, pleasant fragrance, and commitment to covering her aurat (intimate parts of the body), reinforces the narrative's impact, particularly on the perception of women's roles within these extremist ideologies. The narrative for female recruits often highlights the perceived importance of their contribution to the larger cause, fostering a sense of empowerment within the confines of extremist ideology.

This gendered narrative extends its reach into the realm of terrorist financing in Indonesia, where women play a noteworthy role in fundraising and logistical efforts. The Abu Ahmed Foundation, established by the widow of Asep Setiawan, a former member of the terrorist group Jemaah Anshorut Tauhid (JAT) who migrated to Syria and was killed in 2015, exemplifies the active participation of women in supporting terrorist activities. Beyond familial ties, they engage in managing social-humanitarian initiatives, facilitating the flow of funds and aid to extremist groups. In short, women play a crucial and impactful role in the wider landscape of terrorist financing in Indonesia that are driven by narratives carefully crafted to resonate with their unique perspectives and experiences.

These groups not only compensate the families of jailed or slain terrorists but also present a facade of community assistance through philanthropic narratives. Under the guise of foundations or charitable organisations, they solicit donations, exploiting people's empathy while concealing the true destination of the funds. The dual narrative of glorifying violence and camouflaging terrorist activities as benevolence plays a pivotal role in shaping the distorted ideology that propels individuals towards radicalisation and violent extremism.

The deliberate segmentation of the grand narrative based on gender reflects a nuanced understanding of societal dynamics and cultural expectations. By tailoring their messages to specific demographics, extremist groups aim to create a more comprehensive

and inclusive narrative that resonates with diverse segments of the population. The gendered narrative becomes a tool for these groups to expand their reach, influence, and support base, tapping into existing societal structures and expectations to further their ideological goals.

Targeting Female Migrant Workers

Female migrant workers are particularly vulnerable in digital spaces where violent groups like ISIS are active. Social media has enabled Indonesian migrant workers in Hong Kong to connect with and contribute to transnational extremist networks.

The case of Ika Puspitasari, who was convicted in 2017 of funding terrorist activities and planning attacks in several cities, is instructive. Then 36 years old, Ika had worked in Hong Kong from 2004 to 2016, and was in Malaysia from 1997 to 2002. Her online radicalisation process can be viewed through a gendered lens. It also illustrates the impact of **connective action**, which is the idea of someone connecting with a specific narrative online without any direct involvement with the group promoting that narrative (Bennett, 2013).

Ika's journey represents a distinct form of radicalisation that occurs predominantly in the online sphere. Her engagement with ISIS narratives, despite not being part of the offline network, showcases the transformative power of online platforms in shaping individual beliefs and behaviours. Her story also highlights the evolving dynamics of gendered narratives within violent groups like ISIS on social media. The connective action facilitated by these platforms allows women, traditionally under-represented in such networks, to actively participate and contribute to extremist ideologies. Indeed, the shifting landscape of gendered roles within online radicalisation now emphasise the unique opportunities for women like Ika.

Radical groups tailor their messages to resonate with the specific experiences of migrant women. For instance, the narratives might highlight the injustices faced by women in their home countries or current place of residence, presenting radicalisation as a pathway to justice and empowerment. They may also offer roles that give the women a sense of importance and purpose, such as being a part of a larger, heroic struggle.

At a macro level, Ika's case also underscores the global reach and influence of connective action in shaping extremist narratives. Ika's story is not unique. Migrant workers like her are particularly vulnerable to radicalisation due to their social, economic, and emotional challenges. Digital platforms become a lifeline, providing a sense of community and belonging that they might lack in their host countries.

Extremist groups thus craft narratives that play a crucial role in radicalising migrant workers by addressing their unique struggles and offering solutions framed as a greater cause.

Listyowati, a migrant worker in Hong Kong, was radicalised online by a supporter of a radical group in Indonesia, who engaged here with personalised content, giving her a strong connection to the cause. She was persuaded to donate money and planned to travel to the Middle East to participate in armed conflict, lured by a prospective partner through social media.

Global events like conflicts, social movements, and political upheavals significantly influence the radicalisation process by providing context and urgency to the narratives pushed by radical groups. The conflict in the Middle East, for example, is used as a backdrop to recruit individuals, portraying it as a righteous battle that requires support and participation.

Countering the gendered narrative calls for a targeted approach that addresses the unique vulnerabilities and motivations of both men and women within susceptible communities. By deconstructing and challenging the gendered narrative, counterterrorism strategies can disrupt the appeal and recruitment tactics employed by extremist groups, ultimately undermining their ability to garner support based on gender-specific messaging.

FOUR DEADLY NARRATIVES

In the intricate web of narratives that intertwine personal stories, group agendas, and overarching ideologies, a complex narrative landscape unfolds, influencing not only individual decisions but also the financial structures that sustain terrorism. Central to the effectiveness of these movements is not merely their utilisation of media technology, which is increasingly accessible and cost-effective, but also

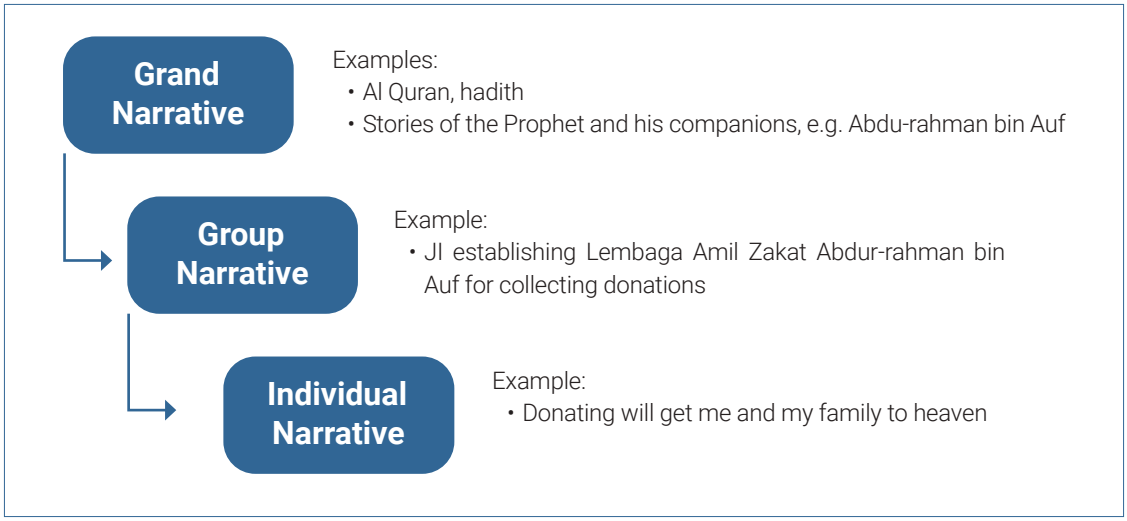


Figure 1. Levels of Narratives

their skill in crafting and disseminating compelling grand narratives.

Furthermore, the financial networks that sustain terrorist organisations are tied to these narratives. Charitable donations, illicit funding streams, and even state sponsorship are often motivated by a shared belief in the grand narrative propagated by these groups. Thus, by leveraging the emotional resonance of their narratives, terrorist organisations not only attract recruits but also secure the financial resources needed to sustain their operations.

In essence, the narrative landscape surrounding terrorism is multifaceted and dynamic, encompassing personal narratives, group strategies, and overarching ideologies, as illustrated in Figure 1. Understanding and disrupting this narrative ecosystem is essential to countering the allure of extremism and dismantling the financial networks that fuel terrorism.

Research for this article has identified four deadly narratives used by JI and JAD and the counter-narrative strategy the authorities should consider.

1.Fighting Groups Considered Enemies of Religion

In this narrative, JI and JAD's adversaries are portrayed as impediments to Islamic law, fostering an "us versus them" mentality. The grand narrative positions the struggle as part of a global mission for an idealised Islamic society.

⇒ To counter this, reframing is crucial, shifting the narrative from divisiveness to one promoting coexistence and understanding.

2. Helping to Fund "Jihad"

This narrative equates financial support with spiritual merit, elevating indirect contributions. The grand narrative establishes a virtuous cycle where financial support becomes a form of spiritual jihad.

⇒ The reframing challenge lies in portraying financial support as detrimental to both the supporter's and society's well-being.

3. Supporting Families of Convicted Terrorists

Positioning support for families as a virtuous act while exploiting familial ties for strategic purposes characterises this narrative. The grand narrative perpetuates the notion of an enduring extended family despite external pressures.

⇒ Reframing involves portraying familial support as a hindrance to genuine rehabilitation efforts.

4. Spreading Group Teachings and Encouraging Jihad

Encouraging individuals towards minimal engagement by framing it as a fundamental expression of faith is the role of this narrative. The grand narrative establishes an overarching theme of jihad as a continuous struggle for a righteous cause.

⇒ Reframing necessitates portraying jihad as a pursuit of peace and personal growth rather than violence.

RECOMMENDATIONS

Tackling these four deadly narratives requires a nuanced understanding and a comprehensive approach that extends beyond immediate circles, delving into the realms of grand narratives, reframing techniques, and manipulative strategies, both online and offline.

Online spaces provide fertile ground for manipulative narratives, thriving on anonymity and exploiting echo chambers and algorithms. Yet offline spaces cannot be disregarded, as manipulative narratives have infiltrated educational institutions, shaping beliefs through biased curricula. Reframing involves dismantling manipulative narratives, exposing their falsehoods, and promoting critical thinking. The proposed solution involves a literacy-based religious moderation programme within Islam.

However, the research also acknowledges the formidable challenge of preventing terrorism funding through legal business methods. A report by the Financial Transaction Reports and Analysis Centre (PPATK) highlights the prevalence of legal routes employed by terrorist groups. These include fundraising through the sale of personal assets owned by terrorists or their families, fundraising by individuals or groups working abroad, and fundraising through *infaq* and *sadaqah* (charitable donations) distribution networks using conventional methods. This nuanced analysis underscores the imperative of adopting comprehensive strategies to curb the multiple dimensions of terrorist financing.

Ultimately, we have to rebuild awareness among stakeholders on the following critical aspects:

Firstly, we need to recognise humans as **homo narrans**, meaning creatures inherently inclined towards storytelling. Particularly pronounced in oral cultures where literacy takes a backseat, the pervasive influence of narratives in shaping human understanding and beliefs cannot be denied. These stories, often challenging to validate logically, acquire significance as they provide affirmation and validation, addressing life's profound questions. For instance, during the emergence of HIV/AIDS, narratives from religious traditions, like the story of the people of Prophet Luth, were used to validate opinions linking the epidemic to divine punishment. Understanding this narrative-driven human nature becomes crucial in addressing and countering narratives that fuel terrorist funding.

Secondly, **credible voices**, especially those of former perpetrators and their families, play a pivotal role in preventing community involvement in terrorist funding. Credible voices wield influence by dispelling misconceptions and shedding light on the deceptive narratives that manipulate public sentiment. A nuanced approach to gender relations within families, considering the active role of wives in fundraising during the incarceration of ex-perpetrators, is also imperative.

Furthermore, narratives that inspire faith or evoke emotional responses can lead individuals to donate without awareness of the true destination of funds. To counter this, **public education** becomes paramount, stressing the importance of thorough scrutiny before making donations. Gender aspects must be incorporated into this educational effort, recognising potential differences in how women and men perceive and approach charitable giving.

Educating the public necessitates an understanding that the complexity lies not only in the meticulous preparation of ways to conceal links between fundraising and terrorism but also in the crafting of narratives that legitimise these actions. Tackling this multifaceted challenge requires a concerted effort to unravel the intricacies of these narratives and build a counter-narrative that promotes transparency, critical questioning, and informed decision-making in charitable contributions.

The public should also be made aware of the use of narrative warfare, especially on social media, to misdirect them. For example, radical groups divert the demand for transparency in charitable giving through slogans such as "The important thing in donating is to be sincere", "Is it so *complicated* to donate?", and "Want *jannah* (heaven)? Let's give alms". The problem is that such narratives are also used by institutions that are active in collecting *infaq* (altruistic spending) and *sadaqah* (charity) funds that are truly for the needs of education and da'wah.

In today's digital era, the race to raise funds creatively and innovatively such as utilising social

media seems to have become a mindset in the community. Mistakes in choosing the beneficiaries of giving need to be rectified immediately. We must educate people that donating is not just a matter of being "sincere" for merit, but it must also be complemented with rigour so that it is not misused.

ABOUT THE AUTHOR

Noor Huda Ismail
is an author, filmmaker, activist, and self-described "repentant journalist" with a desire to tell a larger story about terrorism, foreign fighters and why people join violent organisations. He joined the S Rajaratnam School of International Studies at the Nanyang Technological University as a Visiting Fellow after completing his PhD at Monash University, Melbourne, on an Australian Award Scholarship. In 2005, he was awarded the United Kingdom's Chevening Scholarship to pursue a Master's degree at St Andrew's University, Scotland. While conducting fieldwork in Northern Ireland, he had an epiphany after meeting with a local activist trying to integrate former terrorists into society. On his return to Indonesia in 2008, he established the Institute for International Peace Building to help the social rehabilitation and re-integration of convicted Indonesian terrorists by employing them upon their release in social enterprises such as Dapoer Bistik Solo, a cafe he set up in Central Java. In 2013, he was elected an Ashoka Fellow by the Washington DC-based Ashoka Foundation for being a leading social entrepreneur championing innovative new ideas that transform society. One of his innovations, a community website (www.ruangobrol.id) that allows ex-terrorists to tell their stories, won an Intercultural Award from Austria in 2022. Ismail's documentaries include Jihad Selfie, Pengantin (The Bride), Seeking The Imam and Cubs of the Caliphate. His latest book, *The Deadly Narrative of Terrorism Finance in Indonesia*, will be published in 2024.

REFERENCES

Bennett, W. Lance. 2013. The Logic of Connective Action: Digital Media and the Personalization of Contentious Politics. Cambridge: Cambridge University Press.

Dijk, C. van. (1981). *Rebellion under the Banner of Islam: The Darul Islam in Indonesia*. The Hague: Martinus Nijhoff.

Haleem, M.A.S. Abdel, trans. (2016). *The Qur'an*. New York: Oxford University Press.

Karso. (August 22, 2022). Interview with the Author. Semarang.

Maan, A.K., and P. Cobaugh. (2018). *Introduction to Narrative Warfare: A Primer and Study Guide*. California: Narrative Strategies LLC.

Masykur, Hadi. (2022, October 17). Interview with the Author. Semarang.

Schulze, K.E. (2018). "The Surabaya Bombings and the Evolution of the Jihadi Threat in Indonesia", in *CTC Sentinel*, Vol. 11, Issue 6, pp. 1-6.

Tarrow, S. (2022). *Power in Movement: Social Movements and Contentious Politics (fourth edition)*. Cambridge University Press.

Taufiqurrohman, M. and V. Arianti. (2014). "The 'Anti-Deradicalization' Movement of Indonesian Terrorist Networks" in *Counter Terrorist Trends and Analysis*, Vol. 6, Issue 3, pp. 11-17.

Trofimov, Y. (2008). *The Siege of Mecca: The Forgotten Uprising in Islam's Holiest Shrine*. London: Penguin Books.

Wijayanto, Para. (2022, August 28). Interview with the Author. Jakarta.

WILL WE HELP OTHERS IN A TERRORIST ATTACK?

UNDERSTANDING CRISIS RESPONSES USING A PSYCHO-SOCIAL LENS

Pamela Goh
Singapore University of Social Sciences

ABSTRACT

Terrorist attacks are highly emotional and threatening events, much so when they are characteristically motivated by a perpetrator's intent to harm. Research has shown that being cognisant of this malice precipitates people to focus on personal safety – although it does not simultaneously lead to a reduced inclination to help. Why does the knowledge of an underlying malice encourage people to be more self-oriented, yet still leaves a possibility that they will render critical assistance to others? This paper illuminates, from a psycho-social perspective, the rationality behind human behaviours during a terrorist attack, where risk and threat are omnipresent.

BEING PROSOCIAL DURING DANGER

Humans have historically been described as being selfish in emergencies, of not taking action in everyday settings, such as when witnessing school bullying (Fluke, 2016), or during major crises such as acts of terrorism or violence (Ellebrecht & Joval, 2022; Schillinger, 2014). This perspective is largely guided by the classic concept of bystander effect exemplified by the 1964 murder of Kitty Genovese in New York where neighbours ignored Genovese's screams in the quiet night (History, 2021). With the Genovese case forming the core of their research, Darley and Latané (1968) called the lack of helping in critical situations the bystander effect.

The bystander effect asserts that people are less likely to intervene when others are present, based on the belief that others will take up that responsibility instead (Darley & Latané, 1968). This effect is believed to be more pronounced when more people are around, since the "responsibility" to act is diffused across more individuals.

On the other hand, prosocial behaviour is any deliberate but voluntary action to benefit other people (Eisenberg & Miller, 1987). Mass emergencies and crises are typically accompanied by either a real or perceived sense of mortality for individuals, impacts multiple people concurrently, and offers restricted opportunities to get away (Drury, 2018; Quarantelli, 2001). The nature of crises such as terrorist attacks makes helping in such situations unique from those displayed in everyday life.

It is essential to note that helping during crises is diverse and can range from extreme acts of heroism such as directly interceding to stop an attacker, to simpler compassionate, altruistic acts including helping others to find lost ones or pulling others along during one's escape (Goh, 2019). While prosocial actions both extreme and simpler in nature may present some form of personal risk to the helper, heroism is still primarily a distinct concept from compassionate and altruistic behaviours (Franco et al., 2018). The term hero is often associated with individuals who not only take on physical risks that serve no benefit for oneself, but also risks that are purely unjustifiable (Franco et al., 2011).

Experts on crowd psychology during crises have always recognised the imperative of witnesses and bystanders intervening to reduce both injuries and fatalities (Hamby et al., 2016; Kirschenbaum & Rapaport, 2020). In recent years, interestingly and

fortunately, research has begun to demonstrate that the bystander effect may not be an entirely valid explanation for modern day behaviours during real-life emergencies and non-emergencies. For instance, the collective effort of a group of bystanders can help individuals to overcome the sense of vulnerability based on perceived safety in numbers, making bystander action possible in the presence of other people instead (Philpot et al., 2020).

In Singapore, the 2022 Beach Road slashing incident is a reminder to reconsider the validity of the bystander effect, or bystander inaction, specifically (Wan, 2022). Contrary to being passive, bystanders – including employees of a nearby restaurant – tried to defend the victim from the armed attacker by throwing objects at him from a relatively safe distance (Chia, 2022). Albeit not a terrorist attack, this act of violence shares a commonality with acts of terrorism – there were malevolent individuals attempting to harm others.

Where intentional attacks caused by malicious attackers are concerned, an important question in relation to human selflessness remains. In the presence of an active perpetrator determined to cause maximum harm or death, specifically in a terrorist attack where anyone and everyone is a target, does the likelihood of prosocial behaviour in the acute phase of the crisis reduce? Helping in this context does not necessarily have to refer to heroism; being prosocial can encompass any form of response that attempts to help and benefit other people other than the helper himself or herself.

WHAT AFFECTS THE DECISION TO HELP?

Crises often create significant losses (Shupp et al., 2017), and helping others present a potential risk to the helper's own personal interest. While danger is an indispensable facet of life, evolutionary psychology states that the most adaptive responses to crises involve avoiding the engagement of behaviours, objects, situations, or locations that are clearly threatening (Lindström et al., 2016).

Identity of Recipients

Early explanations of prosocial behaviour, particularly in relation to evolutionary psychology, were predominantly concentrated on kin selection and reciprocity. The former describes self-sacrificial behaviours as a result of wanting to protect and benefit those genetically related, as this contributes to the fitness of one's own genes (Eberhard, 1975). However, kin selection has been criticised for its inadequate applicability, especially in instances of altruism where helping is directed to others without relation to the helper (Foster et al., 2005).

Others have argued that, on the contrary, the influence of external factors has been more substantial than genetic relatedness (Birch & Okasha, 2015). Reciprocity, then, might be a more appropriate explanation for prosocial behaviour. The concept of reciprocity states that altruism in reality can be directed towards non-kin members, except that the relationship between both the helper and recipient must be longstanding enough so that helpers are not exploited and that the act of receiving can be returned in favour (Yamamoto & Tanaka, 2009).

In the grand scheme of things, bystander action contradicts evolutionary origins and confers no benefits to the helper since reacting and intervening in a dangerous situation only threatens their personal survival (Livermore et al., 2021). This is not surprising, and witnesses' accounts, videos, and images of terrorist attacks have also recorded countless acts of self-preservation behaviours by victims such as fleeing and hiding (e.g., 2016 Nice truck attack, Katz & Walt, 2016; 2022 Buffalo mass shooting, Freytas-Tamura & Petri, 2022; Zitser, 2022).

In any time-constrained environment where everyone faces an equal exposure to possible death, do direct intervention (if any) by individuals to help one's own kin, or others beyond either themselves or their familiar persons? It makes no absolute nor moral sense to ignore the plight of a kin just to benefit strangers, since one's available resources are limited. Developmentally, humans have also been taught to behave prosocially particularly towards their in-group, and to always direct critical resources towards kin than non-kin members (Chalik & Dunham, 2020; Olson & Spelke, 2008). In fact, research has revealed that people are generally evaluated more negatively when they fail to help their family members than when they fail to do so for strangers (McManus et al., 2020).

More importantly, people do desire affiliation even amid escape to safety (Mawson, 2005), and this positions the presence and welfare of loved ones as a prime concern. Victims in the 2016 Nice truck attack, such as in the case of Timothe Fournier, for instance, have tragically lost their lives in a bid to protect their family ("Nice attack", 2016). During the 2016 shooting scare at JFK Airport, passengers also tried to search for and contact loved ones in the midst of chaos (Marcius & Schapiro, 2016; Wallace-Wells, 2016). The distress attributted to the separation from familiar figures can be more significant than the physical danger of being caught in a terrorisst attack, and research has suggested that being in the presence of familiar others can exert a calming effect on victims during threats (Cocking et al., 2009; Mawson, 2005).

Would people help others in a terrorist attack? It is a notion conceivable despite the existence of danger, but the identity of the recipient of help matters. Ensuring the well-being of loved ones is likely to take precedence over that of strangers – and people are willing to go as far as persisting in a situation of danger, if it means being able to remain in proximity with loved ones or others with whom they have a close relation (Levine et al., 2005).

Uncertainty in a Situation

Making choices in times of uncertainty means coming to a decision without complete knowledge and thus control of the likely outcomes of the chosen behaviour (Mushtaq et al., 2011). Uncertainty is a central component of crises and has detrimental consequences on the experience of distress (Afifi et al., 2012), yet humans need to be in the know or know what to expect in order to impose order and regain some form of control (Gordon, 2003). For instance, most people fear taking the airplane more than travelling on roads by cars even though land travel has caused more deaths than air travel. The disparity in fear stems from not just the potential catastrophic nature of an airplane incident, but also the uncertainty and relative lack of control over such a situation, and thus their chances of survival (Starr & Whipple, 1980).

Terrorist attacks are a form of psychological warfare aimed at striking fear, uncertainty, and chaos in a society (Butler et al., 2003; Waxman, 2011). It can be challenging to properly assess and understand these events when there is no specific target or modus operandi (Sinclair, 2017), and how attacks unfold and end may completely differ from how it began ("Westminster attack," 2017). Estimating the probability of an attack during a terrorism risk assessment has been posited as one of the most difficult tasks to complete (Levine, 2012).

The lack of helping or intervention by others is associated with, among various factors, the failure to determine that help is necessary in a situation (Oster-Aaland et al., 2009) and one's perceived self-efficacy (Krieger et al., 2017). According to Latané and Darley (1970), several prerequisites need to be in place for helping to emerge, and this includes recognising that an event is indeed an emergency, someone in distress needs help, and the potential helper feels capable enough to intercede. The issue is that uncertainty is a key driver in ensuring that these conditions successfully take place (Pugh, 2016).

Self-efficacy reflects a person's confidence to effectively manage a situation or to undertake a task (Acquadro Maran et al., 2023), and is influenced by information deriving from various sources (Lee & Bong, 2023). In a progressive environment without ample or accurate details to comprehend what is transpiring, it is presumptuous to assume that those caught in danger concurrently feel efficacious enough to know what to do, much less intervene. Furthermore, the likelihood of helping is bolstered by one's previous experiences of intervention in similar circumstances (Krieger et a., 2017). While, and fortunately, not many have direct experience with an act of terrorism, this also means that knowledge and efficacy to help in attacks can be restricted given an absence of prior exposure.

The state of uncertainty can be deleterious since it shapes individual and thus overall crowd behaviours. People are inclined to use emotional and behavioural cues from others (i.e., social influence) to make judgements on how they should best react when they are unsure of what to do (Gigerenzer, 2008; Haghani & Sarvi, 2017). As "ignorant bystanders look at other ignorant bystanders" to determine and emulate the most optimal behavioural response (Burn, 2009, p.781), this observational learning indicates that individuals are unlikelier to help when others are

not seen to be helping, and vice versa (le Bon, 2009; Nook et al., 2016). If most witnesses or victims evaluate an event to not be severe and that it is not a situation where intervention is appropriate, this observed consensus will inhibit the overall crowd from perceiving the situation as an emergency and thus act (Latané & Darley, 1968).

Uncertainty hampers interpretation of an attack and one's ability to determine the needs of others in the same event (Proulx & Fahy, 2003). In other words, if confused individuals are not aware that a terrorist attack is taking place and assistance can be critical for others, this lack of recognition and subsequent inaction can become widespread. A lower probability of helping is hence expected.

Perceived Severity of Crisis

Man-made crises, such as that of terrorist attacks, are perceived to be more threatening and serious than natural and inevitable disasters. Various studies have supported this assertion, such as that of Rudski and colleagues (2011) in which breaking a leg from a car accident is perceived to be more painful than doing so during a hike, and that of Gray and Wegner (2008) in which electric shocks believed to be administered intentionally are rated as more painful than when believed to be administered without human intent. These subjective perceptions are, in reality, not unfounded. Medical research has determined that terror-related injuries are more life-threatening than when caused by a comparable but non-terror-related incident, even if these injuries are similar (Aharonson-Daniel et al., 2003).

Critically, recognising that crises are caused by humans have negative implications on prosocial behaviours. Zagefka et al.'s 2011 study on helping in the aftermath of a crisis discovered that people are more likely to donate to victims of a famine caused by natural drought than to victims of a famine caused by an armed conflict. The motivation driving this discrepancy in desire to help comes from humans' inclination to blame others for their misfortunate – and hence likelier to help those in the drought-famine circumstance given that they are "truly innocent" – even though neither group caused the event nor asked for it to occur (Zagefka et al., 2011). How does this finding, however, relate to helping in the acute phase of a crisis, particularly in a terrorist attack?

Emotions play a fundamental role in influencing behaviours, and humans are instinctively motivated to self-protect (Rogers, 1975, 1983). Fear has a much considerable effect on people and can amplify the level of threat assessed by those caught in an attack (Slovic & Peters, 2006), especially if they are not knowledgeable or skilled to respond to such an event (Pachur et al., 2012). This visceral, innately driven experiential system acts as a critical source of information that facilitates determination of whether a situation is safe or unsafe, thereby helping individuals to effectively navigate a world that is fraught with threats (Slovic & Peters, 2006). Emotions, compounded by the cognitive processes that concurrently occur to facilitate assessing of threat levels, change behavioural inclinations in those caught in danger (Moors, 2020).

Terrorist attacks put people in physical peril, generating the experience of extreme emotions including extreme fear and anxiety (Johnson & Tversky, 1983; Misslin, 2003). Crises trigger significant fear and anxiety in people, and these negative feelings guide the manifestation of survival strategies so that threats will be avoided (van den Berg, 2009). Self-protective reactions in people, including running and hiding in places of safety, are likelier than helping others since they help people to avoid or reduce any uncomfortable physical or psychological feelings of heightened mortality (Ashkenazy & Ganz, 2019; Stern, 2010).

Perceived severity of a crisis is negatively associated with prosocial inclinations (Liebst et al., 2018). The more severe or threatening people consider a crisis or terror attack to be, the less inclined are they to intervene and assist others. A terrorist attack itself is a threatening event; consequently, the expected dominant crowd behaviour in those affected is self-oriented responses, not one that is prosocial in nature.

Presence of Malice in a Terrorist Attack

A distinguishing characteristic of terrorist attacks from other man-made crises is a perpetrator's

deliberate decision and intent to harm. Research findings including neuroimaging results have revealed that the actual experience of pain inflicted by the actions of others is much more intense when individuals perceive malice in these actions (Eisenberger et al., 2003; Gray, 2012). Critically, the mere recognition that malice is the reason for a mass emergency directly deepens perceived threat and severity of the event (Crossley, 2008).

A sense of self-control, or power, is necessary for humans to overcome an instinct for self-interest and thus display prosocial, cooperative behaviours (DeWall et al., 2008). Unfortunately, being subjected to the malicious behaviours of others forcefully imposes a condition of power imbalance between the perpetrator and victim. Any feelings of ability to choose how one behaves, the situations in which one is in, as well as the outcomes that one is trying to achieve, are eroded (Karos et al., 2018).

Prosocial behaviours hinges on power, or, alternatively, the capacity for self-determination (Joosten et al., 2015). With reduced power, consequently, people's behavioural tendencies are impacted since the inhibition to act in a self-oriented manner – albeit necessary for personal survival – becomes challenging to do so. In other words, the instinctive inclination to act in a proself manner is greater than any conscious propensity to be prosocial.

The effect of malice and how it increases the perceived threat or severity of a terror attack has also been empirically proven. In a vignette experiment conducted by Goh (2023), participants reported significantly different levels of threat perception and behavioural inclinations to an intentional vehicle attack versus a non-intentional vehicle accident. Relative to those in the vehicle accident, participants in the vehicle attack perceived the event to be more intentional and threatening, and were thus more inclined to be proself. Interestingly, participants were not necessarily any less prosocial in the vehicle attack than in the vehicle accident.

Being aware that malice is the cause of an attack incites people to be more self-oriented, but research findings nevertheless still reflect hope since a focus on one's own preservation does not correspond to a simultaneous reduction of tendencies to help others. Simply perceiving that a crisis is malicious has significant effects on how victims respond. A crisis is an emotional event to begin with, but a malicious one is inevitably more serious and menacing.

CONCLUSION

The heroism of humans during mass emergencies and crises, specifically in the context of terrorist attacks, has been documented in many media reports (e.g., Holland, 2023; Long, 2017). Such was the case in the 2017 Las Vegas attack – termed the most deleterious mass shooting incident in America's modern history – where Jonathan Smith rushed approximately 30 individuals to safety and took a bullet to his neck (Long, 2017). During the 2019 London Bridge attack, Steve Gallant along with two other witnesses prevented the armed attacker from harming others and escaping until authorities arrived (Bowcott, 2020). In today's era of predominant self-interest (Drury, 2018), heroism observed in these various terrorist incidents does not conform to modern norms especially when intervening is extremely deleterious for the helper.

Will humans help each other in a terrorist attack? Possibly, for the selflessness of humans has been captured both in media reports of terrorist attacks as well as in academic works. It is imperative to note, however, that there are conditions or processes to account for in order to observe human altruism in times of danger.

Personal safety and survival will naturally remain as the topmost priority for people, for the simple reason that a crisis means danger and helping generally comes with risks to oneself. Returning to the example of the Beach Road slashing incident in Singapore, help was indeed rendered to the victim but saving her comprised throwing objects from a distance away from the armed attacker.

Individuals' perception of an on-going terrorist attack essentially has implications on their subsequent responses. Recognising that malice serves as the reason for the attack, and that everyone is an equal target renders the experience a highly serious and threatening one. Self-oriented rather than prosocial, other-oriented responses are more plausible and expected. Nonetheless,

behaviours are contagious, and using others as a tool to sense-make during uncertainty and ambiguity indicates a possibility for widespread helping to occur. Once this uncertainty is reduced and people come to comprehend not just the event but also its severity, however, this perception is likely to become the dominant influence on human behaviours during the crisis. Prosocial responses may still emerge, but their manifestation will be secondary to self-preservation.

ABOUT THE AUTHOR

Pamela Goh
is a lecturer with the Public Safety and Security Programme, at the Singapore University of Social Sciences. Previously from the Ministry of Home Affairs, she specialises in understanding the human psychology behind national security related events, having examined how people behave, communicate, and react in times of offline and online crises. Pamela has a Ph.D in Psychology, and has also presented her thesis on prosociality during intentional crises at the Society for Personality and Social Psychology Annual Convention 2022.

REFERENCES

Acquadro Maran, D., Butt, M. U., & Begotti, T. (2023). Pro-environment behaviors, efficacy beliefs, perceived individual and social norms: A questionnaire survey in a sample of young adults from Pakistan. *SAGE Open, 13*(4), 1-12.

Afifi, W. A., Felix, E. D., & Afifi, T. D. (2012). The impact of uncertainty and communal coping on mental health following natural disasters. *Anxiety, Stress & Coping, 25*(3), 329-347.

Aharonson-Daniel, L., Waisman, Y., Dannon, Y. L., Peleg, K., & Israel Trauma Group. (2003). Epidemiology of terror-related versus non-terror-related traumatic injury in children. *Pediatrics, 112*(4), e280-e280.

Ashkenazy, S., & Ganz, F. D. (2019). The differentiation between pain and discomfort: A concept analysis of discomfort. *Pain Management Nursing, 20*(6), 556-562.

Birch, J., & Okasha, S. (2015). Kin selection and its critics. *BioScience, 65*(1), 22-32.

Bowcott, O. (2020, January 7). Prisoner reveals role in tackling London Bridge attacker with narwhal tusk. *The Guardian*. https://www.theguardian.com/uk-news/2020/jan/07/prisoner-steve-gallant-reveals-role-in-tackling-london-bridge-attacker-with-narwhal-tusk

Butler, A. S., Panzer, A. M., & Goldfrank, L. R. (Eds.). (2003). *Preparing for the psychological consequences of terrorism: A public health strategy*. The National Academies Press.

Burn, S. M. (2009). A situational model of sexual assault prevention through bystander intervention. *Sex Roles, 60*(11), 779-792.

Chalik, L., & Dunham, Y. (2020). Beliefs about moral obligation structure children's social category-based expectations. *Child Development, 91*, e108–e119.

Chia, O. (2022, April 19). 'I heard her shout: Save me, my hand is gone': 9 commended for fending off Beach Road attacker. *The Straits Times*. https://www.straitstimes.com/singapore/courts-crime/i-heard-her-shout-save-me-my-hand-is-gone-9-commended-for-fending-off-beach-road-attacker

Cocking, C., Drury, J., & Reicher, S. (2009). The psychology of crowd behaviour in emergency evacuations: Results from two interview studies and implications for the Fire and Rescue Services. *The Irish Journal of Psychology, 30*(1-2), 59-73.

Crossley, C. D. (2008). Emotional and behavioral reactions to social undermining: A closer look at perceived offender motives. *Organizational Behavior and Human Decision Processes, 108*(1), 14-24.

Darley, J. M., & Latané, B. (1968). Bystander intervention in emergencies: Diffusion of responsibility. *Journal of Personality and Social Psychology, 8*(4), 377-383.

DeWall, C. N., Baumeister, R. F., Gailliot, M. T., & Maner, J. K. (2008). Depletion makes the heart grow less helpful: Helping as a function of self-regulatory energy and genetic relatedness. *Personality and Social Psychology Bulletin, 34*(12), 1653-1662.

Drury, J. (2018). The role of social identity processes in mass emergency behaviour: An integrative review. *European Review of Social Psychology, 29*(1), 38-81.

Eberhard, M. J. W. (1975). The evolution of social behavior by kin selection. *The Quarterly Review of Biology, 50*(1), 1-33.

Eisenberg, N., & Miller, P. A. (1987). The relation of empathy to prosocial and related behaviors. *Psychological Bulletin, 101*(1), 91.

Eisenberger, N. I., Lieberman, M. D., & Williams, K. D. (2003). *Does rejection hurt? An fMRI study of social exclusion. Science, 302*(5643), 290-292.

Ellebrecht, N., & Joval, A. (2022). Active violent incident: Medical first responders' perception of people's willingness to help. *Médecine de Catastrophe-Urgences Collectives, 6*(4), 241-246.

Foster, K. R., Wenseleers, T., & Ratnieks, F. L. (2006). Kin selection is the key to altruism. *Trends in Ecology & Evolution, 21*(2), 57-60.

Fluke, S. M. (2016). *Standing up or standing by: Examining the bystander effect in school bullying* (Order No. 10139916). Available from ProQuest Dissertations & Theses Global (1821965291).

Franco, Z. E., Allison, S. T., Kinsella, E. L., Kohen, A., Langdon, M., & Zimbardo, P. G. (2018). Heroism research: A review of theories, methods, challenges, and trends. *Journal of Humanistic Psychology, 58*(4), 382-396.

Franco, Z. E., Blau, K., & Zimbardo, P. G. (2011). Heroism: A conceptual analysis and differentiation between heroic action and altruism. *Review of General Psychology, 15*(2), 99-113.

Freytas-Tamura, K. D. & Petri, A. E. (2022, May 14). 'Bodies were everywhere.' Witnesses describe Buffalo shooting scene. *The Seattle Times*. https://www.seattletimes.com/nation-world/bodies-were-everywhere-witnesses-describe-buffalo-shooting-scene/

Gigerenzer, G. (2008). Why heuristics work. *Perspectives on Psychological Science, 3*(1), 20-29.

Goh, P. (2019). Against the norm: The act of helping during violent extremist attack. In M. Khader, L.S., Neo, J. Tan, D.D. Cheong, & J. Chin (Eds.), *Learning from violent extremist attacks: Insights for Practitioners and Policymakers* (pp. 359-374). World Scientific Publishing.

Goh, P. (2023). *The effects of perceptions of a malicious intent to harm on victims' prosocial intentions during a crisis*. Doctoral thesis, Nanyang Technological University, Singapore.

Gordon, K. (2003). The impermanence of being: Toward a psychology of uncertainty. *Journal of Humanistic Psychology, 43*(2), 96-117.

Gray, K. (2012). The power of good intentions: Perceived benevolence soothes pain, increases pleasure, and improves taste. *Social Psychological and Personality Science, 3*(5), 639-645.

Gray, K., & Wegner, D. M. (2008). The sting of intentional pain. *Psychological Science, 19*(12), 1260-1262.

Haghani, M., & Sarvi, M. (2017). Following the crowd or avoiding it? Empirical investigation of imitative behaviour in emergency escape of human crowds. *Animal Behaviour, 124*, 47-56.

Hamby, S., Weber, M. C., Grych, J., & Banyard, V. (2016). What difference do bystanders make? The association of bystander involvement with victim outcomes in a community sample. *Psychology of Violence, 6*(1), 91.

History. (2021, May 21). *Kitty Genovese*. https://www.history.com/topics/crime/kitty-genovese

Holland, K. (2023, September 27). Fishmongers' Hall: Attack hero proud of Queen's gallantry award. *BBC*. https://www.bbc.com/news/uk-england-northamptonshire-66927972

Johnson, E. J., & Tversky, A. (1983). Affect, generalization, and the perception of risk. *Journal of Personality and Social Psychology, 45*(1), 20-31.

Joosten, A., van Dijke, M., van Hiel, A., & De Cremer, D. (2015). Out of control!? How loss of self-control influences prosocial behavior: The role of power and moral values. *PLoS ONE, 10*(5), e0126377.

Karos, K., Williams, A. C. D. C., Meulders, A., & Vlaeyen, J. W. (2018). Pain as a threat to the social self: A motivational account. *Pain, 159*(9), 1690-1695.

Katz, M. & Walt, V. (2016, July 15). At least 84 dead after truck crashes into crowd in Nice, France. *TIME*. https://time.com/4407268/nice-attack-france-truck-bastille-day/

Kirschenbaum, A. A., & Rapaport, C. (2020). Helping behavior by bystanders: Contrasting individual vs social contextual factors. *International Journal of Disaster Risk Reduction, 50*, 101816.

Krieger, H., Serrano, S., & Neighbors, C. (2017). The role of self-efficacy for bystander helping behaviors in risky alcohol situations. *Journal of College Student Development, 58*(3), 451.

Lee, H. J., & Bong, M. (2023). Self-efficacy. In R. J. Tierney, F. Rizvi, & K. Erkican (Eds.), *International Encyclopedia of Education* (4th ed., pp. 250–257). Elsevier Science.

Levine, E. S. (2012). Estimating conditional probabilities of terrorist attacks: Modeling adversaries with uncertain value tradeoffs. *Risk Analysis: An International Journal, 32*(2), 294-303.

Levine, M., Prosser, A., Evans, D., & Reicher, S. (2005). Identity and emergency intervention: How social group membership and inclusiveness of group boundaries shape helping behavior. *Personality and Social Psychology Bulletin, 31*(4), 443-453.

Liebst, L. S., Heinskou, M. B., & Ejbye-Ernst, P. (2018). On the actual risk of bystander intervention: A statistical study based on naturally occurring violent emergencies. *Journal of Research in Crime and Delinquency, 55*(1), 27-50.

Lindström, B., Selbing, I., & Olsson, A. (2016). Co-evolution of social learning and evolutionary preparedness in dangerous environments. *PloS one, 11*(8), e0160245.

Latané B. & Darley J. M. (1970). *The unresponsive bystander: Why doesn't he help*. Appleton-Century-Crofts.

le Bon, G. (2009). *Psychology of Crowds*. Sparkling Books Ltd.

Livermore, J. J., Klaassen, F. H., Bramson, B., Hulsman, A. M., Meijer, S. W., Held, L., ... & Roelofs, K. (2021). Approach-avoidance decisions under threat: the role of autonomic psychophysiological states. *Frontiers in Neuroscience, 15*, 621517.

Long, H. (2017, October 3). He was shot helping people during the Las Vegas shooting. His heroics helped his photo go viral. *The Washington Post*. https://www.washingtonpost.com/news/post-nation/wp/2017/10/03/he-helped-people-escape-from-the-storm-of-gunfire-in-las-vegas-now-he-has-a-bullet-in-his-neck/

Marcius, C. R., & Schapiro, R. (2016, August 17). Passengers inside JFK during 'terrifying' shooter scare blast Port Authority for 'chaos'. *New York Daily News*. https://www.nydailynews.com/2016/08/17/passengers-inside-jfk-during-terrifying-shooter-scare-blast-port-authority-for-chaos/#

Mawson, A. R. (2005). Understanding mass panic and other collective responses to threat and disaster. *Psychiatry, 68*(2), 95-113.

McManus, R. M., Kleiman-Weiner, M., & Young, L. (2020). What we owe to family: The impact of special obligations on moral judgment. *Psychological Science, 31*(3), 227-242.

Mills, J. (2020). The global bystander effect: Moral responsibility in our age of ecological crisis. *Journal of Futures Studies, 25*(2), 61-76.

Misslin, R. (2003). The defense system of fear: Behavior and neurocircuitry. `(2), 55-66.

Moors, A. (2020). Appraisal Theory of Emotion. In V. Zeigler-Hill & T.K. Shackelford (Eds.), *Encyclopedia of Personality and Individual Differences* (pp. 232-240). Springer International Publishing AG.

Mushtaq, F., Bland, A. R., & Schaefer, A. (2011). Uncertainty and cognitive control. *Frontiers in psychology, 2*, 249.

Nice attack: Who were the victims? (2016, August 19). *BBC*. https://www.bbc.com/news/world-europe-36805164

Nook, E. C., Ong, D. C., Morelli, S. A., Mitchell, J. P., & Zaki, J. (2016). Prosocial conformity: Prosocial norms generalize across behavior and empathy. *Personality and Social Psychology Bulletin, 42*(8), 1045-1062.

Olson, K. R., & Spelke, E. S. (2008). Foundations of cooperation in young children. *Cognition, 108*, 222–231.

Oster-Aaland, L., Lewis, M. A., Neighbors, C., Vangsness, J., & Larimer, M. E. (2009). Alcohol poisoning among college students turning 21: Do they recognize the symptoms and how do they help? *Journal of Studies on Alcohol and Drugs, Supplement*, (16), 122-130.

Pachur, T., Hertwig, R., & Steinmann, F. (2012). How do people judge risks: Availability heuristic, affect heuristic, or both? *Journal of Experimental Psychology: Applied, 18*(3), 314-330.

Philpot, R., Liebst, L. S., Levine, M., Bernasco, W., & Lindegaard, M. R. (2020). Would I be helped? Cross-national CCTV footage shows that intervention is the norm in public conflicts. *American Psychologist, 75*(1), 66–75.

Proulx, G., & Fahy, R. F. (2003). Evacuation of the World Trade Center: What went right. *CIB REPORT*, 27-34.

Pugh, B., Ningard, H., Ven, T. V., & Butler, L. (2016). Victim ambiguity: Bystander intervention and sexual assault in the college drinking scene. *Deviant Behavior, 37*(4), 401-418.

Quarantelli, E. L. (2001). Panic, sociology of. In N. J. Smelser & P. B. Baltes (Eds.), *International Encyclopedia of the Social and Behavioural Sciences* (pp. 11020–11023). Pergamon Press.

Reysen, S., & Levine, R. V. (2014). People, culture, and place: How place predicts helping toward strangers. In P. J. Rentfrow (Ed.), Geographical Psychology: *Exploring the Interaction of Environment and Behavior* (pp. 241–260). American Psychological Association.

Rogers, R. W. (1975). A protection motivation theory of fear appeals and attitude change. *The Journal of Psychology, 91*(1), 93-114.

Rogers, R. W. (1983). Cognitive and physiological processes in fear appeals and attitude change: A revised theory of protection motivation. In J. Cacioppo & R. Petty (Eds.), *Social Psychophysiology* (pp. 153-176). Guilford Press.

Rudski, J. M., Osei, W., Jacobson, A. R., & Lynch, C. R. (2011). Would you rather be injured by lightning or a downed power line? Preference for natural hazards. *Judgment and Decision Making, 6*(4), 314-322.

Schillinger, T. (2014). *Bystander effect and religious group affiliation: Terrorism and the diffusion of responsibility*. Doctoral dissertation, Walden University.

Shupp, R., Loveridge, S., Skidmore, M., Lim, J., & Rogers, C. (2017). Risk, loss, and ambiguity aversion after a natural disaster. *Economics of Disasters and Climate Change, 1*(2), 121-142.

Sinclair, J. (2017, June 20). *Has terrorism changed us?* wbur. https://www.wbur.org/cognoscenti/2017/06/20/psychology-of-terrorism- justin-sinclair

Slovic, P., & Peters, E. (2006). Risk perception and affect. *Current Directions in Psychological Science, 15*(6), 322-325.

Starr, C., & Whipple, C. (1980). Risks of risk decisions. *Science, 208*(6), 1114– 1119.

Stern, M. D. (2010). Patrimony and the evolution of risk-taking. *PloS one, 5*(7), e11656. van den Berg, M., Fort, R., & Burger, K. (2009). *Natural hazards and risk aversion: Experimental evidence from Latin America* (No. 1005-2016-79151). International Association of Agricultural Economists.

Wan, W. (2022, April 30). Commentary: Beach Road incident shows bystander effect is sometimes a myth. *CNA*. https://www.channelnewsasia.com/commentary/beach-road-chopper-bystander-effect-social-media-kindness-2655671

Wallace-Wells, D. (2016, August 15). Scenes from the terrifying, already forgotten JFK Airport shooting that wasn't. *New York Intelligencer*. https://nymag.com/intelligencer/2016/08/the-terrifying-jfk-airport-shooting-that-wasnt.html

Waxman, D. (2011). Living with terror, not living in terror: The impact of chronic terrorism on Israeli society. *Perspectives on Terrorism, 5*(5/6), 4-26.

Westminster attack: What happened. (2017, April 7). *BBC*. https://www.bbc.com/news/uk-39355108

Yamamoto, S., & Tanaka, M. (2009). How did altruism and reciprocity evolve in humans? Perspectives from experiments on chimpanzees (Pan troglodytes). *Interaction Studies, 10*(2), 150-182.

Zagefka, H., Noor, M., Brown, R., de Moura, G. R., & Hopthrow, T. (2011). Donating to disaster victims: Responses to natural and humanly caused events. *European Journal of Social Psychology, 41*(3), 353-363.

Zitser, J. (2022, May 15). Buffalo mass shooting eyewitnesses describe running for their lives as bullets flew in the suspected racist attack on a grocery store, per reports. *Business Insider*. https://www.businessinsider.com/buffalo-mass-shooting-eyewitnesses-said-they-prayed-as-bullets-flew-2022-5

WHAT DOES IT MEAN TO MAINSTREAM GENDER INCLUSION IN PREVENTING VIOLENT EXTREMISM AND COUNTER TERRORISM?

Gazbiah Sans
PVE Works, Singapore

ABSTRACT

This article aims to define gender inclusion in the preventing violent extremism (PVE) and counter-terrorism (CT) sectors. It is important to have a genuine basis for understanding the impact of gender inclusion and gender mainstreaming, especially in fragile, conflict and violent (FCV) contexts, where women and girls experience acute vulnerabilities, while simultaneously recognising men, boys and marginalised communities are also impacted by violent extremism and terrorism. This article investigates what it means to meaningfully and mindfully gender mainstream in the PVE and CT sectors for communities affected by violent extremism and terrorism. The analysis uses desk research and lived examples to highlight where preventing violent extremism and counter terrorism policies and interventions could be improved.*

VIOLENT EXTREMISM AND TERRORISM ARE GENDERED ISSUES

Societal power imbalances are widely recognised as contributing factors to violent extremism and terrorism. Women and girls, men, boys and marginalised communities are affected differently, underscoring how their individual and gendered experiences can often influence their involvement in violent extremist or terrorist activities. Women and girls, for instance, not only play multifaceted roles as facilitators, attackers, recruiters, and supporters of terrorist groups, but frequently also fall victim to conflict-related sexual violence or are objectified by policymakers as tools to prevent violent extremism and terrorism. Their preexisting limited access to socioeconomic opportunities also exacerbates their vulnerability. In volatile environments, their voices are marginalised and their contributions undervalued, which increase their vulnerability to violence against them (Sans, 2022).

The impact on individuals also vary depending on states' responses, interventions and policies. For example, policymakers often burden women with the responsibility to curb a man's violent extremist actions. This approach not only exploits women's goodwill but widens the chasm of gender inequality, neglecting their rights and security, and ignoring potential repercussions in already volatile settings (Sans, 2022).

All these indicate that violent extremism and terrorism are inescapably gendered phenomena. Yet, attempts to improve gender-based policies relating to preventing violent extremism (PVE) and counter-terrorism (CT) have been largely unsuccessful, not for a lack of information, as numerous scholars have contemplated "women's roles" in violent conflict, but because findings are often not adequately translated into policies (Sans, 2022). Thus, it remains essential to actively consider gendered needs to develop PVE and CT measures that work for everyone.

*This article is adapted from an earlier piece by the author published by the International Affairs Forum titled "Gender Inclusion: What it means to Gender Mainstream in Preventing Violent Extremism and Counter Terrorism?" available on https://www.ia-forum.org/Content/ViewInternal_Document.cfm?contenttype_id=5&ContentID=9827

Defining Gender Inclusion and Gender Mainstreaming

To effectively improve PVE and CT measures, understanding the fundamentals of gender inclusion is necessary. While gender inclusion is not a new concept, understanding it is essential to establish a prosperous society based on equality and equity. Yet there is confusion about what it means. The author's attempts to pinpoint a definition in the literature only found **explanations** for "gender inclusive" or "gender and (social) inclusion". In the context of PVE and CT, much of the literature quickly moved into discussions about mainstreaming and operationalisation of gender inclusion, bypassing the crucial first step of defining gender inclusion itself.

Against this backdrop, the author offers this definition: **Gender inclusion is a process of being gender sensitive by adapting language, behaviours, policies, interventions and mechanisms that provide an equal and equitable landscape for all actors (regardless of sex)**. Here, it is vital to note gender inclusion should not result in being gender neutral or blind, as gender neutrality and blindness tends to perpetuate the existing gender inequalities. Instead, gender inclusion aims for an even-handed manner in PVE and CT measures given that societal power imbalances typically result in women and girls being excluded or ignored. A gender lens is thus required to remove gender biases and stereotypes that perpetuate inequalities (Sans, 2022).

Mainstreaming gender inclusion is essential. The United Nations Office on Drugs and Crime (UNODC, 2020) offers this definition of gender mainstreaming: "[T]he process of assessing the implications for women and men of any planned action, including legislation, policies or programmes, in all areas and at all levels. It is a strategy for making women's as well as girls', boys' and men's concerns and experiences an integral dimension of the design, implementation, monitoring and evaluation of policies and programmes in all political, economic and societal spheres so that women and men benefit equally, and inequality is not perpetrated. **The ultimate goal is to achieve gender equality** [emphasis added]."

CURRENT REALITY

There are a few recurrent themes in states' and international organisations' efforts to introduce gender inclusion into the PVE and CT sectors.

States and international organisations try to have the best of both worlds by linking gender mainstreaming with security and most often, the women, peace and security (WPS) agenda, thus fortifying states' security agenda while simultaneously addressing the gendered consequences of violent extremism and terrorism. These links are further strengthened by insisting that states uphold their human rights obligations, particularly to women and girls. Additionally, there is advocacy for states to use intelligence gathering to potentially identify victims and perpetrators of violent extremism and terrorism; this may, but usually does not, include reports on sexual/gender-based violence (S/GBV), typically prevalent in fragile, conflict and violent (FCV) affected contexts, as such violence is often seen as unrelated or "personal domestic matters".

In practice, therefore, gender mainstreaming is often accompanied by using run of the mill expressions and calls for capacity building, raising awareness, and training of trainers etc., which is jointly carried out with states' consent by international donors and development partners to integrate gender into PVE and CT policies, programmes and activities.

If lived history is an indicator, the current approach to gender inclusion, while seemingly gender inclusive by using a gendered lens, is merely evidencing the lack of action displayed in times of crises. For example, the war in Gaza is having a significant impact on women and girls. As at 12 June 2024, 37,202 Palestinians have been killed, including 15,694 children and 10,367 women (Kuwaiti News Agency, 2024). A report by UN Women dated 19 January 2024 found 70% of the 27,600 civilian fatalities were women and girls, particularly noting: "Women and girls in Gaza are dying at unprecedented levels." It further highlighted that "951,490 women and girls have been displaced from their homes" and "two mothers are killed every hour in Gaza." A 2023 report from the United Nations High Commissioner for Refugees (UNHCR) indicates that "one child is killed every 10 minutes." And yet, what is being done to protect women and children in Gaza?

On the other hand, when the war began in Ukraine in 2022, humanitarian corridors were established for women and children to move to safer locations, and S/GBV awareness and alarms rang to ensure the safety of women and girls, proving that solutions exist and can be implemented. In comparison and similar to Gaza, in other FCV contexts, where violent extremism and terrorism are present, such as Afghanistan, Northern Cameroon, South Sudan, Myanmar, Mozambique, Yemen and Northeast Nigeria, women and girls continue to be subjected to severe forms of abuse, showcasing gross negligence towards and the lack of credibility for gender inclusion in the PVE and CT sectors.

In many instances, gender mainstreaming approaches have been criticised as a "box-ticking" exercise, as the rhetoric espoused fails to match up to the reality on the ground. According to the 2021 "ASEAN Gender Mainstreaming Strategic Framework 2021-2025", there is a "lack [of] political power needed to bring about transformative change for women; and for not being robust enough to counter the multiple sources of backlash against women's rights. As a result, while many governments, development organisations and donors claim a commitment to mainstreaming gender in their policies and programmes, few are implementing it to the degree that is required. There remains a large gap between the rhetoric around gender mainstreaming and actual development and government practice."

Statements such as this are not uncommon and it calls into question the efficacy of gender inclusion practices. Currently, as the ground reality and rhetoric do not match, the general approach to gender inclusion is both disingenuous and promotes lip service. Furthermore, by not giving due recognition to the progress of gender inclusion, both the WPS and gender inclusion agenda are even more weakened. Moreover, it exposes the PVE and CT sectors to "women-washing"—throwing around words related to gender mainstreaming, while overlooking gender-specific vulnerabilities present in the violent extremist and terrorist contexts.

Without an appropriate gender-sensitive lens, PVE and CT policies, programmes and interventions run the risks of muddling programme design, implementation, baseline and endline evaluations, while further frustrating donors and stakeholders who have strong corporate commitments for gender inclusion. Moreover, in protracted crises, when gender inclusion is most needed, we see a failure to act and prevent harm to women and girls. This is due to a lack of willingness to put women and girls at the centre of the discussion during conflicts, hindering mindful and meaningful gender mainstreaming approaches for integrating gender effortlessly and efficiently in PVE and CT policies, strategies, programmes, and interventions.

RECOMMENDATIONS

In order to integrate gender into PVE and CT policies, programmes and interventions and especially in times of crises, a systematic (re) structure that accounts for various levels of organisation at the programmatic levels and within institutional frameworks (i.e., government, international development organisations, NGOs, civil society organisations, academia and the private sector) is needed.

At the programmatic level, considerations that should guide the programme cycle include:

1. In-depth gendered analysis that take into account the local context and use a feedback loop mechanism for *real-time data* to operationalise and integrate gender considerations, while factoring in community ownership and sustainability of programme outcomes.

2. Gendered analysis of the project design, tailoring programme objectives with the needs of women and girls, men, boys and marginalised communities, as identified by communities. This should include a gendered risk assessment and associated mitigation measures to counteract potential bottlenecks in programme implementation and in times of crises.

3. Intentional gender verification milestones at implementation stage to account for gender integration.

4. An accurately identified gender framework for monitoring and evaluation criteria that consider both positive and negative gender dynamics to build on and improve future work.

At the institution level, leading by example means implementing internal policies enabling support for these programmes. For example, basic policies should routinely advocate for gender sensitive employee retention by considering:

1. Committing honestly to gender equality and equity.

2. Establishing human resource policies to achieving gender parity at all levels of employment.

3. Fostering an enabling environment that supports equal pay for equal work.

4. Enhancing the integration of a gender perspective with the aim of removing gender-restrictions or barriers and to improve internal working conditions systematically.

5. Empowering working parents by establishing institutional policies that allow "parental" time-off, rather than penalising or stigmatising the decision to have a family. This should also apply to elderly care.

The idea behind these policy examples is to demonstrate that gender mainstreaming should be achieved at an institutional level with engagement and full participation, in order to have mindful and meaningful gender mainstreaming at the programmatic level. Without the required commitment from senior levels of leadership at institutional levels, the buy-in to implement at the programmatic level is hindered, as it rests on the shoulders of workers, fighting an uphill battle for something they will not receive.

While this is not a substantial list, it provides a basis for gender mainstreaming in PVE and CT programmes by providing a reference point for circumventing unfavourable gender consequences to PVE and CT activities, policies, interventions and programmes. Should such an approach be taken seriously, conditions on the ground, especially in crises, would improve for women and girls, boys, men and marginalised communities.

ABOUT THE AUTHOR

Gazbiah Sans
is the Director of PVE Works. She is a Preventing Violent Extremism and Counter-Terrorism expert, specialising in gender inclusion and gender mainstreaming, specifically in fragile, conflict and violent contexts. She has 15 years of experience, notably with USAID in Cameroon on the Boko Haram affected Lake Chad Basin Region, and with the World Bank in Afghanistan. She serves as the Chair of the Internal Review Panel for the Global Community Engagement and Resilience Fund, the global fund dedicated to preventing violent extremism. She concurrently serves as a core member of the Christchurch Call Advisory Network. She holds a Master's Degree in Global Security/Strategic Studies from Johns Hopkins University.

REFERENCES

ASEAN. (2021, September). ASEAN gender mainstreaming strategic framework 2021-2025. Retrieved from asean.org/wp-content/uploads/2022/01/ASEAN-Gender-Mainstreaming-Strategic-Framework-endorsed-by-AMMW.pdf

Kuwaiti News Agency. (2024, June 13). Death toll of Israeli genocidal war on Gaza climbs to 37,202. Retrieved from www.kuna.net.kw/ArticleDetails.aspx?id=3159984&Language=en.

Sans, G. (2022). Gender biases in preventing violent extremism policies. *International Affairs Forum*. Retrieved from www.ia-forum.org/Content/ViewInternal_Document.cfm?contenttype_id=1&ContentID=9441.

United Nations Office on Drugs and Crime. (2020, December). Mainstreaming gender in terrorism prevention projects/programmes: Briefing notes for staff. Retrieved from www.unodc.org/documents/Gender/20-05713_Terrorism_Brief_ebook_cb.pdf.

United Nations. (2024, January). Facts and figures: Women and girls during the war in Gaza – UN Women. Retrieved from www.un.org/unispal/document/facts-and-figures-women-and-girls-during-the-war-in-gaza-un-women/.

UNHCR. (2023, November). Women bearing the brunt of Israel-Gaza conflict: UN expert. Retrieved from www.ohchr.org/en/press-releases/2023/11/women-bearing-brunt-israel-gaza-conflict-un-expert.

INVISIBLE CHAINS:
AN EVIDENCE-INFORMED STUDY OF PSYCHOLOGICAL COERCION IN HUMAN TRAFFICKING CASES IN SINGAPORE

Stephanie Chan & Kwek Boon Siang
Home Team Psychology Division, Ministry of Home Affairs

ABSTRACT

Psychological coercion is a subtle form of control used by human traffickers to elicit compliance from their victims. A highly favoured method of control used by traffickers, psychological coercion tactics create the "invisible chains" that manipulate and bind victims to their situations. This article is based on a research study commissioned by the Joint Operations Group of the Ministry of Home Affairs, Singapore, to examine psychological coercion that is increasingly prevalent in Trafficking-in-Persons (TIP) cases. Supported by our research data, we have developed a working concept of psychological coercion to aid the efforts of the Interagency TIP Taskforce working to combat human trafficking in Singapore. The acronym TIED-ME aptly encapsulates the five themes we have identified as key to creating the invisible chains compelling forced labour – Trauma Bonding, Isolation, Emotional Distress, Debt Bondage, Manipulation, and Exploitation.

SINGAPORE'S EFFORTS TO FIGHT TRAFFICKING-IN-PERSONS

Trafficking-in-persons (TIP), also known internationally as human trafficking, is a crime that rakes in huge profits, to the tune of USD $236 billion annually for the traffickers, the International Labour Organization (ILO) estimates in a 2024 report. TIP continues to be a global concern with the rise in digital technologies giving traffickers wider reach and easier access to victims.

To combat TIP in Singapore, an inter-agency taskforce on TIP (TIP TF) was established in 2010 and is co-chaired by the Ministry of Home Affairs (MHA) and the Ministry of Manpower (MOM), with representatives from the Singapore Police Force (SPF), the Immigration & Checkpoints Authority (ICA), the Ministry of Social and Family Development (MSF), the Ministry of Health (MOH), the Ministry of Law (MinLaw), the Ministry of Foreign Affairs (MFA), and the Attorney General's Chambers (AGC).

The TIP TF carries out and coordinates anti-trafficking efforts by investigating and prosecuting trafficking cases under the Prevention of Human Trafficking Act (PHTA) and other relevant laws. The PHTA, enacted on 1 March 2015, is complemented by the Women's Charter and Employment of Foreign Manpower Act. It is designed to define acts that constitute abetment of the TIP offence, and criminalising acts of knowingly receiving payment in connection with the exploitation of a trafficked victim. According to the PHTA, "any person who recruits, transports, transfers, harbours or receives an individual (other than a child) by means of (a) the threat or use of force, or any other form of coercion; (b) abduction; (c) fraud or deception; (d) the abuse of power; (e) the abuse of the position of vulnerability of the individual; or (f) the giving to, or the receipt by, another person having control over that individual of any money or other benefit to secure that other person's consent, for the purpose of the exploitation (whether in Singapore or elsewhere) of the individual shall be guilty of an offence." Under PHTA, first offences are punishable with up to 10 years imprisonment, fines up to SGD 100,000 and caning of up to six strokes (PHTA, 2014). Besides enforcement, the PHTA also provides measures for the welfare of trafficked victims and to encourage the reporting of trafficking or suspected trafficking activity.

On 10 May 2021, the Minister for Home Affairs and Law, K. Shanmugam said in Parliament that since the enactment of the PHTA, a total of 260 cases of alleged sex and labour trafficking have been investigated by MOM and SPF, of which 12 cases were prosecuted (Ministry of Home Affairs, 2021).

DEVELOPING AN OPERATIONAL UNDERSTANDING OF PSYCHOLOGICAL COERCION

As part of the TIP TF's long-term commitment to combat TIP, the Joint Operations Group (JOG) of MHA commissioned the Home Team Psychology Division (HTPD) to examine the aspect of psychological coercion that is increasingly prevalent in TIP cases but rarely studied.

The study sought to answer the following questions:

1. What defines psychological coercion?
2. How is it distinguished from physical coercion?
3. What are the explicit and implicit characteristics of traffickers and victims?

The findings have implications for the operational and policy efforts to combat TIP in Singapore. Specifically, the findings we obtained improved and updated operational understanding of psychological coercion in sex trafficking and labour trafficking. It enhanced the criminal justice system pertaining to frontline victim screening and referrals of TIP cases.

Methodology

To obtain a comprehensive understanding of psychological coercion characteristics and tactics in local TIP contexts, the research team applied qualitative research methods to collect, triangulate, and analyse information from multiple sources and the following perspectives:

- Academic Perspective: Comprehensive literature review, inclusive of international studies and screening tools.
- Practitioner Perspective: Eight focus group discussions with local law enforcement agencies and civil society representatives to gather operational experience and expertise.
- Field Research Perspective: Thematic analysis of data in investigation files and qualitative interviews with victims of cases classified as sex trafficking, labour trafficking, and sex vice by the authorities.

Psychological Coercion is a Subset of Coercion

Human trafficking consists of three elements: the act (what is done), the means (how it is done) and the purpose (why it is done). (See Figure 1 for details.)

Coercion is one of the various means used by traffickers to carry out their exploitation. The nature of coercive acts can be overt (i.e., physical coercion) or subtle (i.e., psychological coercion). Psychological coercion and physical coercion are thus both subsets of coercion and a means (how it is done) of human trafficking.

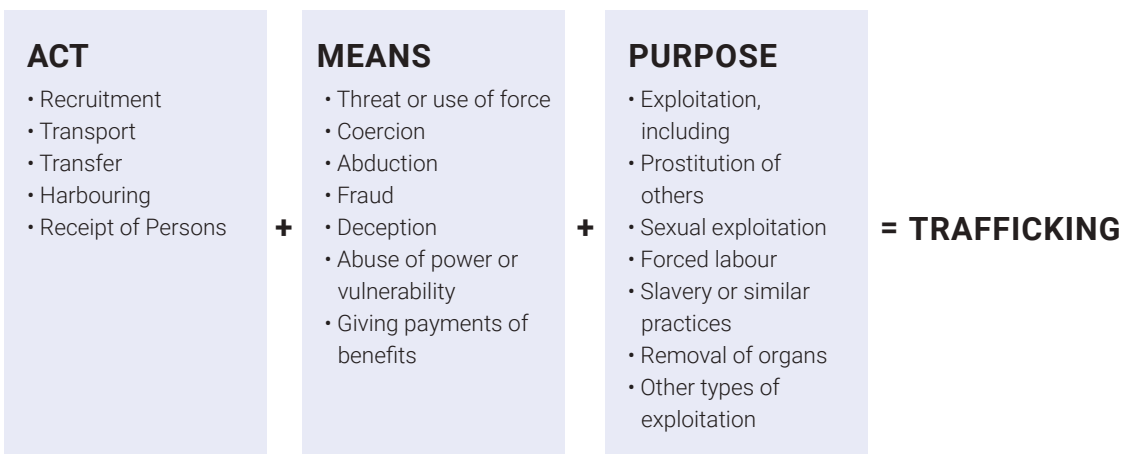


Figure 1. Act, Means and Purposes of Trafficking (United Nations Office of Drugs and Crime)

Defining Psychological Coercion

As the experience of psychological coercion is internal and often subjective, identifying psychological coercion requires an objective standard. At present, there are different ways in which academics, non-governmental organisations, and local and international legislature have defined psychological coercion. In fact, there is overlap in Singapore's and the US's legal definitions of coercion as both countries reference the UNODC model law definition of human trafficking.

UNODC's Definition of Psychological Coercion in TIP, in the UN TIP protocol

a. Threats of harm or physical restraint of any person;
b. Any scheme, plan or pattern intended to cause a person to believe that failure to perform an act would result in serious harm to or physical restraint against any person;
c. Abuse or any threat linked to the legal status of a person; and
d. Psychological pressure.

After a comprehensive review of the definitions of coercion and psychological coercion from 12 established sources,[1] the following six key elements of psychological coercion were derived:

1. Psychological coercion is ***a means*** for traffickers to control and manipulate victims into compliance.
2. ***Patterns and history of violence*** become psychologically coercive such that in the absence of physical violence, compliance is elicited.
3. Psychological coercion is a ***subjective victim experience*** where the victim is made to feel that compliance is the most sensible decision.
4. Traffickers ***exploit their victim's vulnerabilities***.
5. Threats of harm ***can be directed at other individuals*** that the victim is concerned about.
6. Psychological coercion is possible due to ***perceived power differences*** between the trafficker and the victim.

By considering various international viewpoints and consulting local policy and enforcement agencies (i.e., JOG, SPF, ICA, and MOM), we formulated the following working definition of psychological coercion:

Psychological coercion refers to ***subtle means of control*** that traffickers may use to manipulate their victims into compliance. Enabled by the perceived power differences between the victim and the trafficker, traffickers ***exploit victims' vulnerabilities*** to ***create a situation*** in which complying with the traffickers' instructions ***appears to be the most feasible option for the victims***.

HOW DOES PSYCHOLOGICAL COERCION WORK? "INVISIBLE CHAINS" OF CONTROL

Psychological coercion is often referred to as "invisible chains" (Hopper & Hidalgo, 2006) as it does not present with physical abuse despite its significant impact. As discussed by Dando, Walsh and Brierly (2016), "in contrast to historical slavery systems characterized by whips, chains, and physical imprisonment, modern day slavery is less overt, typically with no obvious visible signs of restraint. Rather, psychological abuse and mental manipulation play a powerful role in forcing modern day slaves to work in a variety of industries." As to be expected, this leads to challenges in screening, investigation, and victim care.

How Psychological Coercion Works #1: "Fight-Flight-Freeze"

Psychological coercion elicits compliance by **breaking down the victim's survival responses and thereby their ability to resist and escape the trafficker**. While trauma is commonly associated with physical abuse, non-physical abuse can also be traumatic (Candela, 2016). Victims of trafficking, in an environment with intense stress and unpredictable threats of harm, are often in a state of chronic stress. In response to danger, the body's fight, flight or freeze reactions are activated.

[1]See the first paper of the Home Team Behavioural Sciences Centre (HTBSC)'s TIP report series, *"Understanding Psychological Coercion in Trafficking in Persons"*, available upon request from the author(s).

However, in the case of trafficking, fight or flight responses are often met with further harm. As such, the body 'freezes' and enters a state of what is commonly known as shock, numbing or dissociation (Hopper & Hidalgo, 2006). Furthermore, the resultant chronic stress causes an overactivation of the stress system and as a result, the body undergoes physiological changes to adapt. This reduces the effectiveness of the body's stress response system, lowering the victims' capacity to resist and rendering them into a state of helplessness (Hopper & Hidalgo, 2006). Thus, psychological coercion is often regarded as the method which creates the 'invisible chains' that bind the victim to their trafficker.

How Psychological Coercion Works #2: "Stockholm-Syndrome" Traumatic Bonding

Another way in which the victim is trapped by the abuser is through the development of a traumatic bond. According to Dutton and Painter (1993), **traumatic bonding is a powerful emotional attachment that develops when there is a power imbalance and when the abuser alternates between acts of kindness and coercive behaviour**. In a power imbalanced relationship, the individual with less power will increasingly feel more negative in their self-appraisal and may feel incapable of being independent. The subjugated individual thus increases their dependency on the dominator which then develops a strong affective bond between the person of low power with the individual with high power.

In an abusive relationship interspersed with kindness, **victims may mistake the absence of abuse as gestures of love/kindness** (Crowther-Dowey et al., 2016). Additionally, the alternation between kindness and abuse by the abuser is an intermittent form of reinforcement and punishment. Behavioural psychology research has shown that intermittent reinforcement results in behaviour that is difficult to extinguish (Davey, 1998).

How Psychological Coercion Works #3: "I am Not a Victim"

The coercive tactics employed by traffickers create barriers that impede victim self-identification. Psychological coercion distorts the victim's perception of his or her work and living situation. The following are some examples:

- Some victims may have initially entered the relationship consensually. Being unaware of the deception and coercion by the trafficker, they may not view the relationship as unhealthy (Moore et al., 2020).
- The traumatic bond formed with the trafficker may lead the victim to believe that the relationship is genuine and develop a sense of loyalty to their trafficker. Hence, they may view their provision of sexual service as a gesture for their trafficker (Anderson et al., 2014).
- Due to their guilt and shame, victims may have a distorted sense of self which makes it difficult for them to admit to themselves that they allowed such extortion (Lange, 2011). Instead, victims believe that their prostitution was for their own survival or financial benefit (Anderson et al., 2014).
- Younger victims may not fully grasp the concept of coercion and exploitation (Villacampa & Torres, 2017). Without being able to self-identify, victims are unable to seek help and escape from human trafficking.

Ultimately, the three mechanisms illustrate that psychological coercion manipulates the victim into interpreting their situation as a choice. This form of control is seen in TIP cases as the absence of physical restraints/evidence does frustrate efforts in identifying victims and assessing cases.

TIED-ME – A LOCAL CONCEPTUALISATION OF PSYCHOLOGICAL COERCION

Drawing from academic perspectives, local practitioner observations and field research, characteristics of both psychologically coercive traffickers and their victims, our research identified 5 themes of psychological coercion in TIP cases in Singapore. Specifically, the five themes are **T**rauma Bonding, **I**solation (Psychological), **E**motional Distress, **D**ebt Bondage, and **M**anipulation & **E**xploitation (aka Grooming). Collectively, these themes are conceptualised as the acronym **TIED-ME**, aptly illustrating the invisible chains which TIP victims are subjected to.

5 Themes of Psychological Coercion	
Trauma Bonding	Victims exhibit low self-worth (e.g., "this is what I deserve"), unusual loyalty to the abuser (e.g., "he didn't force me, I chose to do it"), and lack of awareness of this traumatic cycle, in turn, forming an unhealthy bond with trafficker(s).
Isolation (Psychological)	Traffickers isolate the victim(s) psychologically from support and aid.
Emotional Distress	Victims experience fears, doubts, shame, stigma, guilt, indebtedness, misplaced sense of willingness (e.g., motivated by sense of filial piety or duty to financially support their loved ones), and are therefore easily controlled.
Debt Bondage	Traffickers exploit the financial vulnerabilities of victims.
Manipulation & Exploitation	Traffickers utilise both rewards and punishments on the victim(s) repeatedly. This is also commonly known as a grooming process.
Resulting in Victim Compliance	

CONCLUSION

Psychological coercion is a prevalent and subtle means of control used by traffickers to achieve victim compliance. This powerful manipulation exploits victims' vulnerabilities to create a situation in which fulfilling the trafficker's instructions appear to be the most feasible option.

To support Singapore's continual commitment to combatting human trafficking, this research drew from extensive academic expertise, investigation files, and local practitioner experiences to conceptualise a) a local working definition of Psychological Coercion, b) three mechanisms of psychological coercive tactics, and c) **TIED-ME** themes of **T**rauma Bonding, **I**solation (Psychological), **E**motional Distress, **D**ebt Bondage, and **M**anipulation & **E**xploitation (aka Grooming).

There are useful operational and policy implications from understanding traffickers' actions and victims' impact that results in victim compliance. The newly conceptualised TIED-ME can guide victim identification to improve appropriate assistance to victims. It can also be weaved into officer training programmes to enhance operational procedures for case handling and evidence gathering. Psychological coercion can also be introduced as a proof of means of TIP or as an aggravating factor of sex vice or employment infringement for prosecution consideration.

On a broader level, civil society stakeholders can generate outreach materials to improve public awareness and seek public cooperation in combatting TIP. Hence, there are intangible benefits that can be gained from this knowledge on psychological coercion in TIP. To capitalise on the value of the research, Singapore has begun enhancing its operational tools with psychological coercion indicators and conducted its first in-house training on psychological coercion tactics with law enforcement agencies in 2023. Singapore also shared the research findings with ASEAN counterparts at the Singapore-US Third-Country Training Programme (TCTP) 2023.

The research team would like to acknowledge and thank the following coordinating agencies, organisations, and contributors, who have made the completion of this research possible: JOG, SPF, ICA, MOM, MSF, HAGAR Singapore, and EmancipAsia. Special thanks also go to Chief Psychologist of MHA, Dr Majeed Khader; Director, Home Team Psychology Division, Ms. Diong Siew Maan; and former HTBSC colleagues (i.e., Whistine, Joan, Jess, Afreen, John, Shannon, Jannah, Sabrina) for their guidance, support, and encouragement.

ABOUT THE AUTHORS

Stephanie Chan
is a Lead Psychologist with the Home Team Psychology Division (HTPD) of the Ministry of Home Affairs. Stephanie's current research interest is in crime and forensic psychology, with recent research areas on knife crime, youth participation in scams, and the psychology of deception and persuasion, as these have operational applications for cybercrime purposes. Stephanie is a member of the British Psychological Society, and she holds a Master of Science in Forensic Psychology from the University of Leicester in the United Kingdom.

Kwek Boon Siang
is a Principal Psychologist who has been with the Ministry of Home Affairs for more than 15 years. He currently holds the appointment of Deputy Director of the Crime and Forensic Psychology Branch at the Home Team Behavioural Psychology Division (HTPD). His research interests are in violent and sexual crimes, offender risk assessment and rehabilitation, scams, and frontline officers' stress and resilience.

REFERENCES

Anderson, P. M., Coyle, K. K., Johnson, A., & Denner, J. (2014). An Exploratory Study of Adolescent Pimping Relationships. *J Prim Prev, 35*(2), 113-117. https://dx.doi.org/10.1007%2Fs10935-014-0338-3

Candela, K. (2016). Protecting the Invisible Victim: Incorporating Coercive Control in Domestic Violence Statutes. *Family Court Review, 54*(1), 112-125. https://doi-org/10.1111/fcre.12208

Crowther-Dowey C., Gillespie, T., & Hopkins, K. (2016). Building healthy relationships for young people and the prevention of domestic abuse. In V. Bettinson & S. Hilder (Eds.), Domestic Violence: Interdisciplinary Perspectives on Protection, *Prevention and Intervention* (pp. 155-179). Palgrave MacMillan. https://doi.org/10.1057/978-1-137-52452-2_8

Dando, C. J., Walsh, D., & Brierley, R. (2016). Perceptions of Psychological Coercion and Human Trafficking in the West Midlands of England: Beginning to Know the Unknown. *PloS one*, 11(5), e0153263. https://doi.org/10.1371/journal.pone.0153263

Davey, G. C. L. (1998). Learning theory. *Comprehensive Clinical Psychology, 1*, 391-421. https://doi-org.libproxy1.nus.edu.sg/10.1016/B0080-4270(73)00181-4

Dutton, G. A. & Painter, S. (1993). Emotional attachments in abusive relationships: A test of traumatic bonding theory. *Violence and Victims, 8*(2), 105-120.

Home Team Behavioural Sciences (2021). *Understanding psychological coercion in trafficking in persons*. Internal Report.

Hopper, E. & Hidalgo, J. (2006). Invisible chains: Psychological coercion of human trafficking victims. *Intercultural Human Rights Law Review, 1*, 185-209.

International Labour Organization. (2014, March). *Profits and poverty: The economics of forced labour*. *Second edition*, Geneva: International Labour Office.

Lange, A. (2011). Research note: Challenges of identifying female human trafficking victims using a national 1-800 call center. *Trends in Organized Crime, 14*(1), 47-55. https://doi.org/10.1007/s12117-010-9107-8

Ministry of Home Affairs (2021, May 10). Written reply to parliamentary questions on matters related to human trafficking, by Mr. K. Shanmugam, Minister for Home Affairs and Minister for Law [Press Release]. https:/www.mha.gov.sg/mediaroom/parliamentary/written-reply-to-pq-on-matters-related-to-human-trafficking-by-mr-k-shanmugam-minister-for-home-affairs-and-minister-for-law/

Moore, J. L., Houck, C., Hirway, P., Barron, C. E., & Goldberg, A. P. (2020). Trafficking experiences and psychosocial features of domestic minor sex trafficking victims. *Journal of Interpersonal Violence, 35*(15-16), 3148-3163. https://doi.org/10.1177%2F0886260517703373

Prevention of Human Trafficking Act, No 51 of 2014, s 3(3). https://sso.agc.gov.sg/Act/PHTA2014

Villacampa, C., & Torres, N. (2017). Human trafficking for criminal exploitation: The failure to identify victims. *European Journal on Criminal Policy and Research, 23*(3), 393-408. https://doi.org/10.1007/s10610-017-9343-4

CYBERCRIME IN ASEAN:
FOSTERING REGIONAL COLLABORATION

Helena Yixin Huang
S. Rajaratnam School of International Studies, Singapore

ABSTRACT

In today's digital landscape, combatting cybercrime has gained global urgency. With technology's rapid advancement, new opportunities for cybercriminals and law enforcement agencies have emerged. This article examines the complexities of cybercrime, its current state in the Southeast Asia region, and what the Association of South-East Asian Nations (ASEAN) and ASEAN Member States can do to combat cybercrime systematically. The inherently transnational nature of cybercrimes and their interconnectedness necessitates a collaborative framework in the ASEAN region. The framework should include four key pillars: promote information sharing, enhance coordination among law enforcement agencies, facilitate the development of consistent cybersecurity policies and regulations across member states, and enhance capacity building for individuals belonging to the law enforcement and prosecutorial communities. Four additional initiatives are also proposed for a more proactive approach to combatting cybercrime as a region.

THE ASEAN CYBERCRIME LANDSCAPE

In an era of rapid digital expansion, cybercrime has surpassed drug trafficking in profitability globally, becoming a significant issue for many countries. Fuelled by technological advancements, this growth in cybercrime presents a dual challenge as it creates opportunities for criminals while demanding innovative responses from law enforcement. Southeast Asia, a region experiencing significant digital growth, is not spared from the fight against cybercrime.

A fusion of human desires and technical skills exploiting security gaps, cybercrime demands a comprehensive strategy integrating cybersecurity efforts to mitigate threats. With cybercriminals leveraging new technologies such as Artificial Intelligence to enhance their methods, cybersecurity defences must also advance. In addition, tackling cybercrime requires addressing legal and regulatory challenges, laws and jurisdictional discrepancies to improve prosecution and international cooperation.

The Association of Southeast Asian Nations (ASEAN) has been grappling with a rising tide of cybercrime in recent years. One of the key factors contributing to the growth is the rapid expansion of internet connectivity and digital infrastructure. Some of these expansions were driven by the COVID-19 pandemic, while others are ramifications of ASEAN initiatives such as ASEAN Smart Cities Network, the ASEAN Declaration on Industrial Transformation to Industry 4.0 and the ASEAN Digital Masterplan 2025, all of which are aimed at harnessing digital technologies for regional development, integration, and competitiveness of the region.

As more people obtain access to technology, the attack surface for cybercriminals widens, providing ample opportunities and potential victims for them to launch attacks such as phishing, ransomware, and data breaches. The continued quest for digital transformation in the region will continue the trajectory for cybercrime as connectivity increases.

Cybercrime in Developed and Developing Countries

With ten countries of different cultures and levels of development, the type of cybercrime in each ASEAN Member State can vary. It is not

uncommon for cybercrime to evolve in a manner that corresponds to a country's level of technology use, digital infrastructure, and societal behaviour.

In countries where digital literacy and cyber infrastructure might be nascent, cybercriminals often exploit fundamental security gaps, committing crimes such as phishing, primary financial frauds, or viruses that target individuals and small businesses with limited cybersecurity awareness or resources. Due to less sophisticated digital systems and lower awareness, cybercriminals often find exploiting vulnerabilities in these environments easier.

Cybercrimes tend to be more sophisticated in more developed countries with advanced technological infrastructure and widespread internet usage. The high-level integration of digital technology in sectors such as finance and healthcare can present lucrative opportunities for cybercriminals to commit more technical crimes such as advanced persistent threats, large-scale data breaches, and even corporate espionage. Such environment also presents a more profitable target group of victims, such as international corporations and high-net-worth individuals, which can attract sophisticated cybercrime syndicates. This can result in a more organised cybercrime ecosystem that includes dark web marketplaces and Cybercrime-as-a-Service model, where cybercriminals provide their technical expertise to paying customers with malicious intent but who lack advanced technical skills.

Social behaviour and citizens' ability to acquire new skills and technologies can also contribute to the spread of cybercrimes. In countries where e-commerce is highly developed and widely used, there may be a higher incidence of online fraud and identity theft. Conversely, simpler forms of online financial fraud might be more prevalent in countries where digital payment systems are just beginning to gain traction.

Types of Cybercrime across Different ASEAN States

The availability of information on common cybercrimes varies across countries. Although there is no universal definition of what constitutes a "common" cybercrime, it is generally accepted to be determined by the highest number of reported incidents. This understanding is also based on the Singapore Police Force's Annual Scams and Cybercrime Brief, which provides a statistical breakdown of the "common" types of cybercrime in Singapore.

Table 1 is compiled from open sources, including official documents from government entities, news articles, as well as research and industry reports from the private sector. Many of the keywords have been preserved.

Table 1. Sociodemographic Characteristics of the Sample

	Common Cybercrimes
Brunei	Banking scams, online identity theft, social media scams, phone scams
Cambodia	"Cyber slavery", "pig-butchering scams"
Indonesia	Carding, phishing, ransomware, online loans, illegal content
Laos	Scams, cyber fraud
Malaysia	"419", "Macau Scams" Phishing, spam, hacking, cyber bullying or harassment, identity theft, credit card fraud, cyber pornography, virus dissemination, Denial of Service attack
Myanmar	Cybercrime scams (largely targeted at Chinese nationals)
Philippines	Online shopping scam, "Nigerian scam", inheritance scam, overpayment scam, rebate scam, malware, phishing, sexual predation
Singapore	Job scams, e-commerce scams, fake friend call scams, phishing scams, investment scams
Thailand	Call fraud, e-commerce phishing, telephone scams, online scams, online ransom, hacking, sexual harassment, fraud and deception (including fake goods and services, fake part-time job fees, fake loans, fake transfer requests and fake online investments), phishing attempts using fake bank apps, fake online payment platforms, and fake online shopping websites
Vietnam	Online fraud, malware scams, ransomware

A Key Challenge: Inconsistent Categorisations

While information is limited, it is sufficient for a key observation to be made: inconsistencies in the naming and categorising of cybercrimes across ASEAN, which presents a notable challenge in the collective effort to combat the evolving landscape of cybercrime.

This inconsistency is particularly evident when comparing the portrayal of cybercrimes in public discourse – such as news articles and government reports – to the more detailed classifications provided by private sector entities like cybersecurity and insurance companies. Publicly released information tends to focus on cybercrimes which requires lower levels of technical expertise to execute, such as scams, phishing attacks, and other forms of digital fraud. These cybercrimes directly affect the general population, making them of immediate concern to public authorities and, consequently, more frequently reported in the media.

In contrast, industry reports often adopt a more comprehensive view, acknowledging the full spectrum of cyber threats, including those requiring sophisticated technical knowledge to perpetrate, such as ransomware attacks, hacking, and malware deployment. These incidents, while less common in the daily experiences of most internet users, represent significant risks to the integrity of critical infrastructures, corporate data security, and even national security.

One example of the difference in categorisation is the range of vocabulary and terms used across ASEAN states to refer to the same cybercrime. While the same cybercrimes are happening in different states, they are categorised and referred to differently. For example, Malaysia uses terms such as "419" to mean advance fee scams and "Macau Scam" for phone scam calls where the cybercriminal impersonates a public official. "419" is a reference to Section 419 of the Nigerian Criminal Code, which is related to charges and penalties for fraud cases with the modus operandi involving victims making advance payments before they can receive money. This same type of crime is known in Philippines as the "Nigerian scam". This is an example of how cybercrimes are not just categorised into types, but also based on the crime's modus operandi. Another example is "pig-butchering" scams, in which "fraudsters spend months cultivating a relationship with the victims before urging them to invest in bogus investment schemes" (Wong, 2022). Initial contact in "pig-butchering crimes" are usually made through mobile phones and social media platforms, yet Cambodia categories them specifically as "pig-butchering" scams rather than a telephone scam or fraud or deception, which is how Thailand has categorised it, while Singapore classifies it as an investment scam.

Another aspect of variation is the use of "cyber threat" in some situations related to cybercrime. The distinction between what is considered a cybercrime and cyber threat is not merely semantic; it has actual implications on how policymakers, law enforcement, and the cybersecurity community address these issues. Cyber threats encompass a broader category that includes potential risks and vulnerabilities, while cybercrimes are specific illegal activities that exploit these vulnerabilities.

The variance in categorisation can confuse the public, dilute the understanding of cybercrime and cyber risks, and complicate the work of policymakers and researchers. Developing effective countermeasures and policy recommendations becomes more daunting without a unified framework for identifying and classifying cybercrimes. This lack of clarity can hinder accurate data collection, efforts to allocate resources effectively, design targeted awareness campaigns, and implement robust cybersecurity measures.

In addition, the ambiguity in categorisation impacts the ability to identify ownership of cybersecurity issues within governments and organisations. When the boundaries between different types of cyber incidents, cyber threats and cybercrimes are blurred, determining which agency or department is responsible for responding to an incident can become problematic, leading to delays in action or gaps in defence. Recognising patterns in cybercrime helps predict and prevent future attacks, but without precise categorisation, this analytical work will be compromised. This is particularly concerning when considering the potential for

cybercrimes to escalate into threats against critical infrastructure and national security. The ability to discern when a cybercrime evolves into a significant threat is crucial for prioritising responses and mobilising appropriate resources.

Cybercrime Legislation in ASEAN

Cybercrime legislation is essential to providing legal frameworks for effectively prosecuting cybercriminals because the subjects of cybercrime – such as data and system integrity – are often not accounted for in traditional criminal law. As cybercrime cases increase and become more varied, the lack of a cybercrime legislation may allow particular criminal activities to fall into legal grey zones. Establishing legal clarity and uniformity is another critical function of cybercrime laws. Legal clarity is not only essential to law enforcement agencies but also for individuals and businesses who want to understand their rights and responsibilities in the digital domain.

Singapore categorises cybercrime into two distinct categories – cyber-dependent and cyber-enabled crimes. Cyber-dependent crimes are "offences under the Computer Misuse Act (CMA) in which the computer is a target" (Singapore Police Force, n.d.), while cyber-enabled crimes are "offences in which the computer is used to facilitate the commission of an offence" (Singapore Police Force, n.d.). In July 2023, the Singapore Parliament passed the Online Criminal Harms Act, which "introduces measures to enable authorities to deal more effectively with online activities that are criminal in nature" (Singapore Police Force, n.d.).

An example of a case charged under CMA concerned an individual "involved in laundering over S$30,000 from overseas fraud through his and another's bank account in Singapore, distributing the proceeds locally" (Singapore Police Force, n.d.). The individual facilitated fraud by relinquishing control of his bank account to receive funds and accessing another individual's bank account to use it to distribute funds to others in Singapore. The case was charged under the CMA because the individual's actions involved unauthorised access and misuse of computer systems and bank accounts. By handing over his internet banking credentials and ATM card, he allowed unauthorised access to his bank account. Similarly, accessing another person's bank account to withdraw money constitutes unauthorised use of computer services. CMA criminalises such acts of unauthorised access, use, or manipulation of computer systems, particularly when they lead to financial crimes including fraud.

While the lack of cybercrime legislation does not mean that ASEAN states are unable to prosecute cybercriminals successfully, there is no assurance that using the existing non-cybercrime legislation will continue to be effective in the long run. This is especially true of emerging and innovative cybercrimes that arise from new technologies or when dealing with cybercriminals who are conscientious enough to study the legislation for potential loopholes to exploit.

CURRENT ASEAN EFFORTS TO COMBAT CYBERCRIME

In 1999, ASEAN established the Senior Officials Meeting on Transnational Crime (SOMTC), and in 2014, the ASEAN Working Group on Cybercrime was started as part of the cybercrime component of the SOMTC's work programme from 2013 to 2015. In 2017, ASEAN adopted the Declaration to Prevent and Combat Cybercrime, thus reaffirming ASEAN's commitment to "continue working together in the fight against cybercrime through activities aimed at enhancing each member state's national framework for cooperation and collaboration in addressing the misuse of cyberspace" (ASEAN, 2017). An ASEAN Regional Computer Emergency Response Team (CERT) was also established in 2022 to "strengthen ASEAN's overall cybersecurity posture and operational readiness in dealing with the fast-evolving cyber landscape by enabling stronger regional cybersecurity incident response coordination and Critical Information Infrastructure (CII) protection cooperation, including for cross-border CII such as banking and finance, communications, aviation and maritime" (Cybersecurity Agency of Singapore, 2022).

In addition, the INTERPOL Global Complex for Innovation in Singapore is home to the INTERPOL Cyber Capabilities and Capacity Development

Project. Funded by the United States Department of State, the project aims to "strengthen the ability of countries in [ASEAN] to combat cybercrime and to work together as a region" (INTERPOL, n.d.). In terms of capacity building which can also contribute towards tackling cybercrime, the ASEAN-Singapore Cybersecurity Centre of Excellence and the ASEAN-Japan Cybersecurity Capacity Building Centre were set up to build capacities on cyber governance and cyber operations.

Regional Success Stories

Despite the differences and gaps in legislation in member states, there are still success stories from the region. Both Operation Night Fury (2019-2020) and Operation Goldfish Alpha (2019) saw close collaboration between several ASEAN states under the guidance and coordination of INTERPOL's ASEAN Cybercrime Operations Desk. Operation Night Fury was an operation against a malware strain targeting e-commerce websites in ASEAN, stealing victims' personal information and payment details. The Indonesian National Police had turned to the Interpol ASEAN Cybercrime Operations Desk for technical and operational support, culminating in the eventual arrest of three individuals suspected of commanding servers in Indonesia. Unlike Operation Night Fury, Operation Goldfish Alpha was not the result of a technical request from an ASEAN member state. Instead, INTERPOL noticed the rise of cryptojacking (unauthorised use of someone's device or system to mine cryptocurrency) as a cybercrime and garnered national and law enforcement CERTs from all ten ASEAN states to deal collaboratively with existing technical vulnerabilities in the region.

Despite the two episodes of success mentioned above, it should be noted that the cybercrimes in these two operations impacted several states, it was likely due to the scale or intensity of the crimes that INTERPOL was involved. As a region, ASEAN and member states need to learn and build up their own capabilities and capacities to effectively carry out similar operations collaboratively, even if the crimes are on a smaller scale. In other words, ASEAN states cannot depend only on organisations such as INTERPOL to coordinate collaborative contributions in combating cybercrime. To this end, a regional collaborative framework might be the answer.

A REGIONAL COLLABORATIVE FRAMEWORK

Some have pitched the idea of an ASEAN cybercrime legislation for member states to effectively address legal gaps and ensure comprehensive legal measures against cybercriminals. While it is ideal for such legislation to exist, it is undoubtedly idealistic as ASEAN adheres to its principle of non-interference. Rather than assuming such a Sisyphean task is the only solution, it is more pragmatic and efficient for ASEAN to establish a regional collaborative framework on cybercrime. If drawn up strategically, the framework can serve as a roadmap to assist ASEAN states in playing a role to create an ecosystem in ASEAN that can combat and reduce cybercrimes, regardless of which ASEAN country the crime originated or took place in.

For the regional collaborative framework to be effective, it needs to address the different aspects essential to the prevention and investigation of cybercrimes and prosecution of cybercriminals, and it must be robust enough to support the transnational nature of most cybercrimes. This means that the framework should consist of at least four key pillars to promote information sharing, strengthen coordination among relevant agencies, facilitate the development of consistent cybersecurity policies and regulations across ASEAN states, as well as enhance capacity building for individuals belonging to the law enforcement and prosecutorial communities, including investigators, prosecutors and judges. Through these pillars, ASEAN states can leverage each other's strengths to protect their domestic and regional digital ecosystems and critical infrastructures more effectively.

It has to be noted that while some aspects of the four pillars are currently already being implemented by individual states, the impact is crippled if there is no systematic regional framework to guide the process. A regional problem can only be resolved through regional coordinated efforts.

Pillar 1: Promote Information Sharing

The first pillar in the collaborative framework should be to promote information sharing and timely exchange of critical information, including threat intelligence, investigation information, and cybercrime data.

Cybercriminals often exploit gaps in information and communication among countries by strategically selecting targets in different jurisdictions. They also use anonymising technologies to conceal their identities and locations, and target victims and nations according to the varying levels of cybersecurity awareness and capabilities among nations. This makes it essential for ASEAN to establish mechanisms that promote and facilitate the sharing of cybercrime-related information.

Information sharing enables quicker threat detection and response as ASEAN states collectively identify ongoing and emerging cybercrimes, the different types of vulnerabilities facilitating these crimes, and the critical points to commence investigations. This reduces the time window for cybercriminals to operate undetected and helps to minimise the potential impact of cybercrimes. Shared information and intelligence can assist in attributing cybercrime to specific threat actors, making it easier to hold them accountable and potentially deter future crimes. Information sharing can also help ensure a constantly updated and renewed collective knowledge base on cybercrime happenings across the ASEAN states to tackle cybercrime effectively.

By fostering a culture of trust and cooperation in sharing information, ASEAN member states can also improve their ability to detect, respond to, and mitigate cyber threats.

Pillar 2: Strengthen Collaboration among Relevant Agencies

To combat the escalating challenge of cybercrime effectively, ASEAN states must strengthen coordination among organisations ranging from law enforcement to prosecutorial agencies. A factor often leading to the success rate of cybercriminals is gaps in jurisdictions. Cybercriminals often operate in a borderless digital realm, which allows them to evade law enforcement by exploiting jurisdictional complexities. This second pillar, which can take the form of Mutual Legal Assistance agreements, will help to ensure that cybercriminals do not escape justice simply by crossing national borders or when they are not acting from the same geographical boundaries as their victims.

The diverse technological infrastructures and expertise levels across states pose both a challenge and an opportunity. Collaboration among law enforcement agencies enables the pooling of resources, investigative leads, sharing of expertise, and access to advanced technology available in the different ASEAN states. This approach can enhance their collective capabilities in responding to, tracking, and apprehending cybercriminals responsible for cyberattacks, from targeting critical infrastructure to online fraud schemes and pig-butchering scams.

For prosecutorial agencies, closer collaboration can harmonise legal frameworks, making it harder for cybercriminals to exploit jurisdictional discrepancies across ASEAN states. An integral component of this collaborative effort could involve establishing specialised networks dedicated to cybercrime enforcement and prosecution. These networks can serve as platforms to facilitate rapid information exchange and coordination of cross-border legal actions.

Pillar 3: Develop Consistent Cybersecurity Policies and Regulations across ASEAN

The diversity of legal frameworks and cybersecurity policies among ASEAN member states can create vulnerabilities and challenges in addressing cyber threats effectively. The third pillar is to facilitate the development of consistent cybersecurity policies and regulations across ASEAN to establish a robust defence against cybercrime. Securing the channels where cybercrime takes place will inevitably reduce cybercrime occurrences.

Consistency in cybersecurity policies can lead to higher standards of cyber hygiene in the region. Uniform adoption of best cybersecurity practices in areas such as advanced threat detection and response capabilities can elevate the region's overall cybersecurity posture. This alignment would also help address the disparities in cybersecurity awareness and preparedness, ensuring that more developed ASEAN states can assist their less developed counterparts, leading to a collective elevation in cyber defences in the region.

As ASEAN states adopt consistent cybersecurity standards and practices, the region will move

towards closing the gaps and vulnerabilities that cybercriminals often exploit. This collective response mitigates the impact of attacks and makes it more challenging for cybercriminals to find easy targets within the region. In addition, it serves as a deterrent to cybercriminals as they become aware of the increased difficulty in breaching a united front.

By strengthening the region's cybersecurity posture, ASEAN can create a more unified, resilient, and secure digital environment that benefits economies, governments, and citizens.

Pillar 4: Enhance Capacity Building for Law Enforcement and Prosecutorial Communities

The effectiveness of combating cybercrime relies heavily on the expertise and capabilities of law enforcement officers, investigators, prosecutors, and judges. Cybercriminals continually adapt their tactics, demanding continuous learning and adaptation from those responsible for maintaining law and order. Capacity building for cybercrime should encompass comprehensive training in digital forensics, cybersecurity investigations, and the prosecution of cybercriminals.

Access to cutting-edge technology, knowledge sharing, and best practices are essential components of such capacity-building efforts. Elevating the skills and knowledge of individuals within the law enforcement and prosecutorial communities can ensure adequate response to cybercrimes, witness protection, gathering of digital evidence and the prosecution of cybercriminals. By promoting international cooperation in capacity building, the region can collectively raise its level of expertise, creating a more secure environment for all and making ASEAN a less attractive region to be targeted by cybercriminals.

Public prosecutors and judges should also be trained to understand the technicalities affecting the confidentiality, integrity, and availability of digital data submitted as forensic evidence. With the rise in cybercrime, the demand for such members of the prosecutorial team will increase. Capacity building for existing prosecutors and judges can be a quick way to ensure the necessary expertise exists in the individual ASEAN state to handle cybercrime cases effectively, resulting in successful prosecution and sentencing.

INITIATIVES FOR PROACTIVE MEASURES

The proposed collaborative framework will no doubt take time to formulate. In the meantime, ASEAN and member states should consider taking on initiatives that can lead to more proactive measures to tackle cybercrime in the region. These initiatives include determining working parameters and baselines, increasing transparency, involving multiple stakeholders, and increasing data collection related to cybercrime.

Determining Working Parameters and Baselines

ASEAN does not have a published list of what it considers to be a cybercrime. The absence of a standardised understanding of cybercrime within ASEAN presents challenges in fostering a unified approach to combatting such crimes across the region.

The United Nations Cybercrime Convention has played a pivotal role in delineating the contours of what constitutes cybercrime on the global stage. During its negotiation, although there was no agreement on a definition of cybercrime, it still successfully identified a range of cyber-dependent and cyber-enabled offences. These include egregious acts such as online child sexual exploitation, solicitation, terrorism, arms trafficking, the illegal distribution of counterfeit medicines and medical products, and incitement or coercion to suicide.

Throughout the convention's negotiation process, the possibility for ASEAN member states to align with or at least recognise their respective non-negotiable positions in relation to the draft texts was evident. This alignment could facilitate the harmonisation of ASEAN's cybercrime discourse, accelerating progress towards consensus on critical issues and the adoption of a unified regional stance. Establishing such a consensus is crucial for defining international norms and standards that ASEAN can adopt or adapt to enhance regional cooperation on cybercrime.

Adopting parameters in line with those identified in the convention could serve as a critical step towards achieving regional alignment on the issue of cybercrime. Establishing a shared understanding of what constitutes cybercrime is fundamental not only to developing cohesive policy and enforcement strategies but also to creating reliable mechanisms for data collection and analysis. Such metrics are indispensable for accurately assessing the scope, scale, and evolution of cybercrime within the region.

Increasing Transparency

Transparency in discussions concerning cybercrime within the ASEAN region is pivotal for several reasons, particularly as these dialogues tend to occur in Track 1 meetings – closed-door roundtables, ASEAN Senior Officials Meeting on Transnational Crime, and the ASEAN Working Group on Cybercrime – where there is often minimal to no public disclosure of the proceedings. The lack of public disclosure of the proceedings can potentially obscure critical information and hinder the collaborative efforts of ASEAN and member states.

Transparency can play a pivotal role in enhancing public awareness and understanding of cybercrime issues within the region. By providing accessible information on the nature of cyber threats and the strategies employed to combat them, ASEAN can empower individuals and organisations to take proactive measures to protect themselves online. This heightened public awareness is crucial for building a resilient digital culture that values security and privacy, further bolstering the region's defences against cybercrime.

In addition, transparency ensures accountability by allowing for the scrutiny of decisions and actions taken by ASEAN bodies dealing with cybercrime. This scrutiny is essential for assessing the impact and efficiency of cybersecurity initiatives, pinpointing weaknesses, and determining where further resources or adjustments are necessary. By making information available on discussions and agreements, ASEAN can engage a broader range of stakeholders in its cybercrime efforts, leveraging expertise, resources, and innovation from across sectors.

Multi-Stakeholder Engagement

Involving multiple stakeholders in combating cybercrime within ASEAN offers an efficient and holistic approach that enhances understanding of the complex factors contributing to cyber threats in the region. This inclusive strategy ensures that policies and initiatives to counteract cybercrime are comprehensive and deeply rooted in an authentic understanding of the challenges and dynamics at play on the ground. By integrating perspectives from various sectors, these efforts can more effectively address cybercrime.

The value of multi-stakeholder engagement is particularly pronounced in ASEAN, a region marked by a rich tapestry of cultures, economies, and levels of digital maturity. Such diversity demands a nuanced approach to cybersecurity, capable of accommodating and respecting the unique characteristics of each member state while also harnessing domestic cultural strengths. This ensures that regional initiatives are inclusive and adaptive to local contexts and effectively leverage each country's intrinsic capabilities and insights to combat cyber threats more effectively.

Civil society organisations play a crucial role in this ecosystem by providing a grassroots perspective that sheds light on the societal impacts of cybercrime and the common traits of vulnerable victims. Academics enrich this dialogue by offering rigorous analysis and forward-looking insights into the effectiveness of policy measures and their potential impact on cybercrime, national security, and economic stability. Through research and scholarship, they help anticipate future challenges and opportunities, guiding policy and strategy with evidence-based recommendations. Private companies, especially those in the technology and cybersecurity sectors, bring their first-hand knowledge of the latest threats and their investment in cutting-edge security solutions to the table.

Increasing data collection

The importance of data in policymaking cannot be underestimated. As illustrated earlier in this article, the lack of data on cybercrime can be an impediment to the fight against cybercrime. Clear statistics provide the evidence base for developing targeted and effective policies and guide decisions on allocating resources more efficiently. Robust collection of data and strategic use of statistics can provide a quantitative foundation to understand the scope and nature of cybercrime in the region. This involves tracking the frequency, types, and targets of cybercrimes. On top of being instrumental in identifying trends and patterns, the data and statistics collected can be used for developing predictive analysis and pre-emptive measures. For example, a surge of pig-butchering scam cases in the region can be a strong reason for countries with rising wealth to direct resources and prompt more focused investigations and cybersecurity training for the financial industry.

With data and statistics on hand, data analytics can also be used to identify patterns consistent with cybercriminal activities. Anomaly detection algorithms can be utilised to flag activities that deviate from usual behaviour, which is often indicative of cybercrime. It can also be used to predict future trends and the demographics of potential victims. Advanced data analytics can be utilised to monitor and analyse cybercrime marketplaces on the dark web.

Enhancing data collection requires a coordinated effort across ASEAN. Part of the efforts might involve developing a common framework for classifying and reporting different types of cybercrimes to ensure comparability and reliability in the standardisation of data reported. Furthermore, varying levels of technological advancement across the region might pose a challenge to uniform data collection and analysis. Despite this, member states and ASEAN need to devise an effective way of collecting data related to cybercrime to tackle cybercrime pre-emptively and proactively.

CONCLUSION

As ASEAN continues to evolve digitally, cybercrime will continue to be a battle the region has to fight. Effective ways to combat cybercrime will demand a collaborative and proactive response. The need for robust cybercrime legislation, enhanced regional cooperation, and increased investment in cybersecurity infrastructure has never been more critical. ASEAN member states must start prioritising digital defence mechanisms, foster a culture of cyber awareness, and engage in continuous dialogue and information sharing. The fight against cybercrime in ASEAN is not just about protecting digital assets; it's about safeguarding the region's future, economic stability, and the security of its citizens. As ASEAN stands at the pivotal moment of digital innovation and regional progress, its commitment to combating cybercrime will be crucial in shaping a secure, resilient, and prosperous digital landscape for all its members.

ABOUT THE AUTHOR

Helena Yixin Huang
is an Associate Research Fellow with the Executive Deputy Chairman's Office at the S. Rajaratnam School of International Studies (RSIS), Nanyang Technological University, Singapore. A former civil servant, she previously worked in government organisations including the Cyber Security Agency of Singapore, the Attorney-General's Chambers and the Corrupt Practices Investigation Bureau. She holds a Master of Science in International Relations from RSIS. Her research straddles both digital and cyber issues, covering topics such as how the use of digital technologies impacts states and societies, and cybercrime. Helena's recent publications in the RSIS commentaries series include "UN Cybercrime Convention: Relevance to ASEAN" and "Internet Governance: Priority Issues for ASEAN".

REFERENCES

ASEAN. (2017). Declaration to Prevent and Combat Cybercrime. *ASEAN*. Retrieved from https://asean.org

Chang, L. Y. C. (2017). Cybercrime and Cyber Security in ASEAN. In *Comparative Criminology in Asia* (pp. 135–148). Springer International Publishing. https://doi.org/10.1007/978-3-319-54942-2_10

Cyber Security Agency of Singapore. (2021, Oct 6). ASEAN-Singapore Cybersecurity Centre of Excellence. *Cyber Security Agency of Singapore*. Retrieved from https://www.csa.gov.sg

Cyber Security Agency of Singapore. (2022, Oct 20). Establishment of ASEAN Regional Computer Emergency Response Team (CERT). *Cyber Security Agency of Singapore*. Retrieved from https://www.csa.gov.sg

Department of Justice. (n.d.). Primer on Cybercrime. *Department of Justice, Philippines*. Retrieved from https://www.doj.gov.ph

Hypernet. (2023, March 11). There are 5 Types of Cybercrime in Indonesia. *Hypernet*. Retrieved from https://www.hypernet.co.id

Huang, Helena Yixin. (2024, Jan 16). UN Cybercrime Convention: Relevance to ASEAN. RSIS Commentaries Series. Retrieved from https://www.rsis.edu.sg

INTERPOL. (2021, n.d.) ASEAN Cyberthreat Assessment 2020: Key Insights from the ASEAN Cybercrime Operations Desk. *INTERPOL*. Retrieved from https://asean.org

INTERPOL. (2021, n.d.) National Cybercrime Strategy Guidebook. *INTERPOL*. Retrieved from https://www.interpol.int

INTERPOL. (n.d.) ASEAN Cybercrime Operations Desk. *INTERPOL*. Retrieved from https://www.interpol.int

Muharram, Sitti Syamsiar Binti & Suhaimi, Mohd. Zuhairizan & Marcus, Markrandy. (2022). Cybercrimes in Malaysia. Journal of Education and Social Sciences, 22(1), 34-38.

MyGovernment. (n.n.). General Information. *MyGovernment*. Retrieved from https://www.malaysia.gov.my/

Philippine National Police. (2013). Cybercrime Threat Landscape in the Philippines. *Philippine National Police, Anti-Cybercrime Group*. Retrieved from https://acg.pnp.gov.ph

Pratama, Yoga & Sakti, Krisna Indra & Setyadi, Firmawan & Ibrahim, Nur Ahmad Azi & Nur, Ali Mukti. (2022). Cybercrime": The Phenomenon of Crime through the Internet in Indonesia. *International Conference Restructuring and Transforming Law, 1*(1), 294-301.

Podkul, Cezary. (2023, Oct 5). Southeast Asian Casinos Emerge as Major Enablers of Global Cybercrime. Propublica. Retrieved from https://www.propublica.org

Serena in Insurance. (2023, July 7). Cybercrime in Thailand: Current Trends and Solutions. *Pacific Prime Thailand*. Retrieved from www.pacificprime.co.th

Sim, Dewey & Dhillon, Amrit & Azmi, Hadi. (2022, Jan 26). From OCBC phishing to the 'Macau scam', how cyber criminals from Singapore and Hong Kong to Malaysia and India stay one step ahead of the banks. *South China Morning Post*. Retrieved from https://www.scmp.com

Singapore Police Force. (n.d.) Introduction to OCHA. *Singapore Police Force*. Retrieved from https://www.police.gov.sg

Singapore Police Force. (n.d.) Cybercrime. *Singapore Police Force*. Retrieved from https://www.police.gov.sg

Singapore Police Force. (2024, Feb 18). Annual Scams and Cybercrime Brief 2023. *Singapore Police Force*. Retrieved from https://www.police.gov.sg

Singapore Police Force. (n.d.) Man to be Charged for Money Laundering and Computer Misuse Act Offences. *Singapore Police Force*. Retrieved from https://www.police.gov.sg

Turton, Shaun. (2021, Sep 1). Cyber slavery: Inside Cambodia's online scam gangs. Nikkei Asia. Retrieved from https://asia.nikkei.com

United Nations. (2023, Sep 2). Draft text of convention. United Nations. Retrieved from https://www.unodc.org

Vietnam's cyberspace: fertile land for financial crime. (2022, Oct 19). *Vietnamnet Global*. Retrieved from https://vietnamnet.vn/en

Wong, Shiying. (2022, Feb 20). The pig-butchering scam: Con artists who come for your heart and wallet. *The Straits Times*. Retrieved from https://www.straitstimes.com

Yip, Christy & Grosse, Sara. (2023, Oct 23). Every day, half a million malware apps are created for scamming. Who's behind them?. *Channel News Asia*. Retrieved from https://www.channelnewsasia.com

UNDERSTANDING THE PSYCHOLOGY OF INVESTMENT SCAMS:
CASE STUDY OF A PIG-BUTCHERING SCAM VICTIM

Low Eu Hian, Tan Wei Liang, Carolyn Misir & Jansen Ang
Police Psychological Services Department, Singapore Police Force

ABSTRACT

Investment scams have been on the rise in Singapore, becoming the fifth most prevalent and the most financially damaging scam type in 2023. A case study analysis of an in-depth interview with a pig-butchering scam victim was conducted to understand the factors underlying the prevalence of investment scams. The study reveals insights into victim characteristics, psychological vulnerabilities exploited by investment scams, as well as potential warning signs. The theories that surround these factors, the relevant psychological characteristics, as well as the linkages to crime prevention in Singapore are also discussed.

INVESTMENT SCAMS THAT FATTEN, THEN BUTCHER THEIR VICTIMS

Investment scams refer to scams that try to convince investors to make purchases using untrue information. Victims will typically be promised huge profits while being assured that they bear minimal risk (Federal Bureau of Investigation, 2022).

Globally, countries are facing a serious problem with investment scams. The United States has suffered a 127% increase in investment scam cases, with USD$1.45 billion lost in 2021 and USD$3.31 billion lost in 2022. Asian territories such as Hong Kong have also been affected, with HK$148.3 million lost in 2023, up from HK$81.32 million lost in 2022 (Anti-Deception Coordination Centre, 2023).

Investment scams are prevalent in Singapore too and are the most financially damaging scam type in recent years. There were 4,030 investment scams in 2023, a 29.7% increase from the 3,108 cases in 2022. The amount of money lost to such scams also increased by 3.1%, from $198.3 million in 2022 to at least $204.5 million in 2023 (Singapore Police Force, 2024).

Investment scams have clearly caused serious financial damage both locally and globally. To take effective countermeasures, it is critical to understand how investment scams can cause damage.

Some investment scams have incorporated elements from other scam types. For example, pig-butchering scams utilise the relationship element used in internet love scams to gain trust. Scammers attempt to gain victims' trust by becoming their "lover" or "friend" through cordial engagement – akin to fattening up the pig – then gradually convince them to part with increasingly large amounts of their money over time through some fictitious investment scheme – the butchering (see Figure 1 for more details).

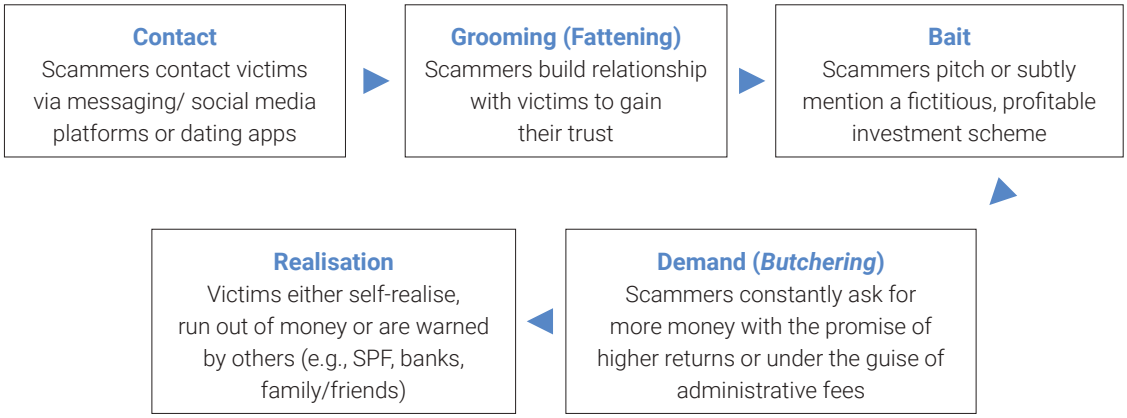


Figure 1. Five-Stage Process of Pig-Butchering Scam

As far back as 2019, pig-butchering scams were already accounting for as much as 60% of all fraud cases in China, with losses exceeding 25% of all fraud losses (Wang & Zhou, 2023). Globally, however, it was only in 2023 that pig-butchering scams were identified as an especially problematic variant of investment scam (North American Securities Administrators Association, 2023), although some law enforcement agencies also classify them as love scams.

However they are classified, pig-butchering scams have proven to be very lucrative for crime syndicates. In 2021, the US recorded losses of at least US$429 million from pig-butchering scams (Federal Bureau of Investigation, 2022). By 2023, the estimated losses had spiked to almost US$4 billion (Rebane & Watson, 2024). A recent study tracking the flow of funds from more than 4,000 victims of pig-butchering scams to crypto exchanges has estimated that scammers likely stole as much as US$75 billion from victims around the world over four years from 2020 to 2024 (Faux, 2024).

An analysis of publicly reported cases in Singapore in 2023 reveals that pig-butchering scams have become especially prevalent here, making up 13 out 18 investment scam cases featured by the National Crime Prevention Council's Scam Alert website (National Crime Prevention Council, 2023). The prevalence of the pig-butchering variant suggests that there is a movement towards more complex investment scams that rely on manipulating the victim over a prolonged period, both on an international and local level. Analysing how pig-butchering scams operate can provide insight into how to tackle the new wave of complex investment scams. Hence, this article focuses on pig-butchering as the variant of interest.

Investment scams can also have severe mental effects on victims. Their personal relationships may suffer, and the experience can be harmful to their mental wellbeing and self-esteem (Bailey et al., 2019). When investment scams involve some attempt to build a fake romantic relationship with the victim, the effects may worsen, with the victim suffering from symptoms similar to post-traumatic stress disorder (Chuang, 2021). In particularly severe cases, the victim may even contemplate suicide (Chuang, 2021). In June 2024, CNN ran a story titled "Killed by a scam: A father took his life after losing his savings to international criminal gangs. He's not the only one." The man featured had committed suicide after falling victim to a pig-butchering scam (Rebane & Watson, 2024).

The damage inflicted by investment scams can be severe. It is therefore important to understand how investment scams operate and how to better prevent them. This paper explores the mechanics behind pig-butchering scams (i.e., decision-making framework, persuasion techniques) and the psychosocial factors influencing an individual's scam vulnerability (i.e., cognitive biases) to support a more comprehensive understanding of investment scams.

PSYCHOSOCIAL VARIABLES ASSOCIATED WITH INVESTMENT SCAMS

Some past studies have focused on the personality traits that may be associated with higher risk of victimisation. For example, impulsivity and neuroticism have been linked to being a more likely victim of online investment scams (Whitty, 2020). These psychological traits reflect some level of emotional instability, which may make these individuals more vulnerable to the emotive cues that scammers commonly employ (Whitty, 2020).

Another study conducted in Japan has also shed light on how the big five personality traits (extraversion, agreeableness, conscientiousness, neuroticism and openness) can also affect the way people approach investment scams, finding conscientiousness to be positively related to a lower probability of falling for a financial scam. Kadoya et al. (2020) hypothesised that individuals with low conscientiousness are less likely to logically appraise offers and are hence more vulnerable to financially-related scams such as investment scams.

In a study comparing 813 general investors and 214 investment fraud victims, materialism and willingness to undertake risky investment behaviours are noted to be characteristics of victims of investment scams (Deliema et al., 2020). These personality traits may make an individual more susceptible to standard persuasion methods used in investment scams, which also makes them more attractive targets for scammers. For example, risk-taking materialistic individuals may choose to ignore how improbable it is that incredible returns can be obtained at low risk as they are blinded by their desire for money (Deliema et al., 2020).

On the other hand, a study by Whitty (2020) has revealed findings that go against common stereotypes about victims of investment scams. Contrary to popular belief, victims are usually well-educated, with the average score being 3.36 on a scale where 1 represents a lower than high school education level, and 5 representing having a doctoral degree (Whitty, 2020). The results contradict the expectation that individuals who are more highly educated can detect scams more easily. This suggests that just being educated is not a sufficient defence against scams and even intelligent people can become victims. Additionally, despite some scam prevention training focusing on protecting women, it is men who are more likely to fall for investment scams, with males making up 64% of victims (Whitty, 2020). Hence it is evident that scam prevention efforts are needed just as much for men, and regardless of gender, more needs to be done to protect individuals. Importantly, individuals with a more internal locus of control have also been shown to be more likely to be victims of investment scams. This may be because their focus on their own actions makes them less sensitive to scam indicators and less willing to acknowledge the ability of scammers to influence their decision making, which makes them more vulnerable (Whitty, 2020).

Effects of Cultural Norms on Victim Susceptibility

Certain cultural norms can make individuals more vulnerable to investment scams. One study has found that subjective norms are a notable predictor of intended behaviours. This suggests that societal pressure from the groups we belong to can play a part in shaping our decisions with regards to investment scams as well (Ajzen, 1991). The effects of cultural norms can be observed within specific contexts. Research into investment scams in Vietnam has shown that communities where trusting relationships are the norm may be more vulnerable to investment scams (Nguyen et al., 2023). For example, in Vietnam if an investment opportunity is recommended by a relative, it is perceived as low risk, which makes it more likely that they will fall for the investment scam as they will not be on guard. Individuals may also find it hard to turn down such scam offers because they do not wish to antagonise those who are close to them (Nguyen et al., 2023).

DECISION MAKING IN INVESTMENT SCAMS

Construal Level Theory is the main theoretical framework that is utilised to explain how decision making is influenced in investment scams. Construal Level Theory suggests that humans are only able to directly experience things in the immediate moment when they occur (Trope &

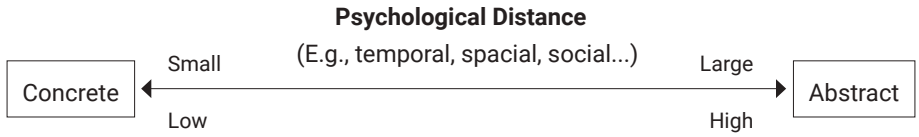


Figure 2. Diagram of Construal Level Theory

Liberman, 2010). Attempting to engage with something that exists beyond an individual's experiences in the present requires them to form a mental construal of it. These mental constructions represent things that are psychologically distant from individuals and serve as a means of transcending their immediate experiences.

Psychological distance is a subjective concept; it takes its reference point from where an individual's current self is positioned. Something that is more psychologically distant is one that is a greater distance away from the position of their current self, whether it is spatially, temporally etc. The greater the psychological distance, the more high-level (abstract) the mental construal becomes, while the shorter the psychological distance, the more low-level (concrete) it becomes instead. This in turn affects the way that an individual makes decisions and engages in different mental processes. When thinking about an investment product, a high-level construal may deal with the overall idea of investing (e.g. save for the future, secure a comfortable life), while a low-level construal will focus on details (e.g. how will the investment work, what are the realistic returns).

When spatial and temporal distance is greater, high-level information is more impactful, while low-level information is given less weightage (Trope & Liberman, 2010). Therefore, big picture theories will impact decision making more than specific details. These two effects can lead to overconfidence when it comes to making predictions regarding psychologically distant events. This occurs because elements that are considered certain in high-level information are overweighted, while elements that are considered uncertain in low-level information are given lesser weight than they deserve.

Using financial products framed as long-term investments as an example, the idea of making huge profits in the future will influence decision making more than specific details about the investment mechanism that suggest that profits may not be as great as advertised. As a result, confidence in expected outcomes for psychologically distant events may be unwarranted, leading to poor decision making.

Construal level effects can alternatively be presented through desirability and feasibility in choices. Desirability deals with the overall expected value that an action produces, therefore it is a feature of high-level construal (Liberman & Trope, 1998). In contrast, feasibility involves dealing with the specific means that are used to achieve something and is thus a feature of low-level construal. Hence, as psychological distance increases, people are more likely to make decisions based on how desirable something is rather than how feasible it is. The danger is compounded by the effect where greater temporal distance makes people more comfortable with uncertain probabilities and outcomes associated with it (Onay et al., 2013), making them even less likely to detect potential issues. This can lead to vulnerability to investment scams as victims may ignore or fail to detect warning signs in pursuit of desired goals such as earning substantial amounts of money.

The **Elaboration Likelihood Model** provides a supplementary explanation of how scammers trick victims into falling for their schemes. Elaboration Likelihood Model suggests that there are two pathways through which people can be persuaded: the peripheral route and the central route (Petty & Cacioppo, 1986).

Under the peripheral route, persuasion is triggered by cues that are largely unrelated to logic. For example, individuals may be persuaded by how attractive the source of the message is. The peripheral route is engaged when an individual lacks the ability or interest to process

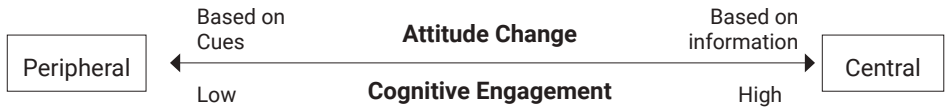


Figure 3. Diagram of Elaboration Likelihood Model

the message. On the other hand, the central route involves thoughtful deliberation of whether there is merit to the information being presented. This involves a high level of cognitive engagement and information is evaluated thoroughly. The central route is engaged when an individual has both the ability and motivation to process a message.

Scammers utilise certain persuasion techniques (e.g. visceral cues, time pressure) that exploit our cognitive vulnerabilities and cause us to utilise our peripheral route. For example, a scammer may engage the principle of scarcity by claiming that an investment is for a limited time only. This can reduce the victim's ability to thoroughly process the scammer's message, as they may rush through their decision-making process out of fear of losing the opportunity that is being presented to them. Hence, they end up engaging the peripheral route and fail to notice that something is amiss.

PERSUASION TECHNIQUES USED IN INVESTMENT SCAMS

Persuasion techniques also directly affect the thought processes of victims. Cialdini's principles of persuasion provide a comprehensive overview of the tactics that can be employed by scammers. They include the following:

Reciprocation refers to how people tend to feel compelled to return favours that have been done for them (Cialdini, 2007). Reciprocity is embedded in all human cultures and is a pillar of a cohesive society, by creating binding ties between members. This principle can be exploited by scammers who begin by offering something to the victim to start things off. For example, they may offer to make an initial deposit on behalf of the victim for the investment, making the victim feel compelled to invest some of their own money to repay the initial favour. This enables scammers to hook in victims who may initially have been reluctant to start investing any of their own money.

Consistency deals with how people possess a desire to remain consistent in the way that they act and behave (Cialdini, 2007). Consistency as a trait is highly valued, e.g. because an individual is seen as being more reliable and honest. Hence, individuals feel compelled to show that they are consistent. This can be very problematic for victims of investment scams as their initial investment may compel them to continue investing as they want to remain consistently committed. In this way, victims may be locked into a vicious cycle where they continue to invest despite many warning signs, resulting in a greater loss than necessary.

Social proof is engaged when we feel the need to look to others and reference what they have done when making our own decisions (Cialdini, 2007). This is especially notable in situations where there is uncertainty about what is the right move to make. Scammers may engage this principle by creating telegram chats where other scammers pretend to be happy customers of the investment scheme. This creates the illusion that the investment scheme must be good as others seem to be actively investing and benefitting from it. As a result, victims may let their guard down and buy into the scam as they are convinced that it must be a legitimate scheme.

Liking is the phenomenon where we are more likely to accept requests from others if we like them on some level (Cialdini, 2007). For example, we may like someone more if they are physically attractive, or similar to us. These various factors that increase liking can be mutually reinforcing which makes liking a particularly powerful effect when manipulated. Pig-butchering scams can make heavy use of this principle as they are structured around forming a deep relationship with the victim. Hence fake but attractive profile pictures are used, and scammers try to make the victim enjoy their company. These elements make the victim more inclined to agree to participate in the investment schemes brought up by the scammer, as they see the scammer as someone likable.

Authority comes into effect because people feel an urge to comply in an almost automatic fashion to instructions from authority figures or even mere symbols of authority (Cialdini, 2007). This occurs even when an individual feels that something is amiss, or they instinctually know that the instructions could be detrimental. Scammers can exploit this principle by pretending to be influential traders or people in positions of power in the financial industry, to compel the victim to obey their directions to invest in the fraudulent schemes. Victims may decide against their best interests to do so as they believe that the scammer must know better than them since they seem experienced and powerful.

Scarcity is a commonly applied principle, and it deals with situations where people more highly value and desire something just because it is less available (Cialdini, 2007). Scammers may exploit this principle by claiming that their offer is limited time only, or open only to a very select group of people. Due to fears of losing out, victims may fail to conduct the appropriate checks and commit without giving themselves enough time to judge the legitimacy of the scheme, leading to them getting tricked by investment scams.

Persuasion techniques are a powerful tool that can be exploited by scammers. Therefore, it is essential that we understand the mechanisms behind these core persuasion techniques in order to develop a method of disrupting their messaging.

COGNITIVE BIASES ASSOCIATED WITH INVESTMENT SCAMS

Cognitive biases are an important area to explore when considering vulnerability to investment scams as they can affect an individual's ability to rationally identify and avoid scams (Wen et al., 2022). The biases explored in this section will be summarised in Table 1 below:

Table 1. Summary of Cognitive Biases

Biases	Explanation
Overconfidence bias	Causes individuals to believe that they have greater than average skills in a particular area, such as investment prowess in the case of investment scams.
Sunk cost fallacy	Individuals continue with a project or decision despite evidence suggesting that it is no longer beneficial, primarily because they have already committed significant resources into it
Near miss effect	Experiencing a close call or narrowly avoiding a negative outcome increases motivation, persistence, and risk-taking behaviour
Optimism bias	Individuals systematically underestimate the likelihood of negative events and overestimate the likelihood of positive events happening to them compared to others
Break even effect	The tendency for individuals to engage in riskier behaviour or continue investing in a decision or project when they perceive themselves as being close to achieving a break-even point
Confirmation bias	Involves ignoring information that contradicts an individual's beliefs, while only paying attention to information that affirms what an individual wants to believe is true
Framing bias	Individuals' decisions or judgments are influenced by the way information is presented or framed, rather than the actual content of the information

Certain cognitive biases play an important role in making an individual more susceptible to making the initial commitment to an investment scam. **Overconfidence bias** is the tendency for individuals to have an unwarranted belief in their abilities, judgements, or predictions, leading them to overestimate their performance or underestimate risks (Oskamp, 1965). This gives them the false confidence that they are likely to be right when making decisions when their judgement may in fact be inappropriate or incorrect. As a result, victims may fail to question obvious problems in the schemes they are caught in and believe what they are told too easily because they believe they are unlikely to be tricked (Pressman, 1998). This may be especially relevant to explaining why educated individuals are getting scammed more frequently, as their education may make them believe that they are more able to detect scams than they really are, leading to a lack of caution.

Optimism bias refers to how individuals tend to underestimate how likely it is that negative events will occur to them, while overestimating how likely it is that positive events will occur to them (Weinstein, 1980). This can make an individual more vulnerable to investment scams as they may overestimate the potential profits they can receive while downplaying the potential losses, which makes them commit to the investment when they should rationally have avoided it (Hidajat et al., 2020).

Framing bias is another powerful tool used by investment scammers. By presenting only the positive information about their investment scheme, the scammers seek to convince investors that the scheme is better than it really is by showing only the benefits. This makes victims more interested in the scheme, making it easier to convince them to make the initial investment that traps them in the scam (Hidajat et al., 2020).

Other biases play a central role in keeping victims ensnared by the investment scam, causing them to continue losing money. One bias that traps victims in investment scams is the **sunk cost fallacy**. In the context of investment scams, when an initial investment has already been made, people are more likely to continue that investment and overweigh how successful that investment has been, even when it is no longer beneficial. This occurs as they believe it would be wasteful if they do not continue (Arkes & Blumer, 1985). This is especially problematic as those who have already been caught in the initial investment scam are unlikely to pull out of them, and instead continue to stick with the scheme and lose even more money. They are also unlikely to be receptive to advice that they have been tricked.

Near miss effect is another bias that can trap individuals in investment scams. This effect occurs when a victim "almost" manages to secure some favourable outcome, such as turning a profit in an investment scam. Instead of seeing this as evidence of failure, victims see it as proof that they almost succeeded, which biases their perspective on how viable this investment scheme actually is (Habib & Dixon, 2010). Hence this may set victims up for yet another round of attempting to gain from the scheme when they should rationally have exited the scheme already after the near miss.

The **break-even effect** applies to individuals who are close to a point where they can recoup their losses. Although a prior loss would normally make an individual more risk adverse, if they are close to a point where they can break even, they will actually become more risk taking instead (Thaler & Johnson, 1990). In the context of investment scams, initial losses can be incurred as a result of fake fees or initial deposits. This in turn can cause victims to engage in more risk-taking behaviour such as continuing to pay fees in order to release their money, even if they may have suspicions that they are being scammed. This behaviour is driven by the belief that once they get their money back, they can break even. Hence, the victim ends up losing more money in a desperate, futile attempt to get back their money and break even.

Confirmation bias refers to how individuals selectively seek, interpret, and remember information that confirms their pre-existing beliefs or hypotheses while disregarding or downplaying contradictory evidence (Nickerson, 1998). This is especially dangerous in the context of investment scams as individuals will actively ignore warning signs that they are being scammed, while choosing to focus on the false

signals that scammers use to make victims think that they are making a profit. This causes them to be unable to identify that they are caught in a scam and hence end up trapped by the scam and losing even more money.

Although it is not possible to erase cognitive biases, understanding how scammers may seek to exploit them provides valuable insight into potential countermeasures.

RESEARCH QUESTION

In the current literature, there are promising psychological theories that can generally explain why victims fall for scams. However, more work must be done to apply these theories and test their applicability on the different variants of scams, particularly on the uprising trend of investment scams. Additionally, most scam-related studies are done in a western context, and there is a dearth of research within an Asian context like Singapore. Hence, this study aims to answer the following research question through a case study analysis: what are the psychological processes and persuasion techniques that affect victims of investment scams, particularly in Singapore?

METHODOLOGY

A comprehensive literature review of the existing research on investment scams was carried out to consolidate theories and information for use in this paper. Subsequently, an exploratory study with a case study approach was undertaken to provide more insights into the mechanisms of investment scams, as well as the psychological factors that influence the victim. A case study approach was chosen as it is particularly beneficial in providing a comprehensive understanding of a contemporary phenomenon of interest in its natural real-world setting (Crowe et al., 2011), which is appropriate in this research context. Additionally, data collected via case study approach tends to be significantly richer and of greater depth compared to experimental designs (Vu & Feinstein, 2017). Hence, an analysis of an in-depth interview with a pig-butchering scam victim was used to better elucidate the victim's cognitive biases and decision-making processes, as well as the persuasion techniques used in an investment scam.

CASE STUDY

Victim Characteristics

Male, bachelor's degree "in information technology", earning "between 120 to 150,000 a year"

The case study supports prior research findings that scam victim characteristics can be very different from common stereotypes. In line with research findings, being highly educated does not provide sufficient protection against being scammed, suggesting that the qualities we associate with being educated may not be particularly effective in scam detection. Furthermore, males do not seem to be any less likely to fall prey to investment scams compared to females, hence some scam prevention training that has traditionally focused on protecting women should be re-evaluated and expanded to support men as well. Victims also do not seem to have to be in financially desperate circumstances to be attracted to the prospects presented by these investment scams. This suggests that the range of potential victims may be far greater than what is commonly expected, since people across a wide range of financial circumstances can all be vulnerable, not just those who are struggling.

Persuasion Techniques and Cognitive Bias

"...this lady got 9 out of 10 times right ... this is not possible ... even I only get 6 out of 10 right."

Various persuasion principles and cognitive biases also come into play in this case study. It is notable that the scammer did not need to introduce themselves as a financial expert to abuse the authority principle, simply appearing to understand how the gold investment worked seemed to be sufficient to convince the victim to follow their instructions, even though fashion design and investment have no relation. Perhaps more vigilance needs to be encouraged, especially when there appears to be a discrepancy between the apparent expertise of the person and what they are claiming.

Authority was also abused when tricking the victim into thinking that the platform used should be safe to use. In this case, the platform introduced to the victim was legitimate, while the brokerage it connected to was not. It is possible that the victim believed that a platform licensed by an authority such as the Monetary Authority of Singapore (MAS) would not expose him to any dangerous scams, hence he did not think to look more deeply into how his fund was being handled. This tells us that it is dangerous to assume that an investment product is legitimate just because the first few components of it are safe to use, and that it is necessary to ensure that every part of the process is being handled as intended.

"...this one is an Oanda account, right? So they're licensed by MAS. ... So what happens is that uh there was another app that we use to transfer, that gives instructions on the website, so the website had a chat function and it gave us bank instructions to transfer money to a certain bank account in Singapore. Right and I did that, not knowing that these are all scammers' accounts...."

The scammer also told him that he could start with just a small amount of money, reflecting use of the foot in the door technique where a small request is made first to make the victim more willing to put up with a larger request due to consistency. This enables scammers to progressively encourage victims to part with increasingly large amounts of money.

"you just need a few hundred dollars to put in"

Furthermore, the victim noted that the scammer had appeared to transfer some of her own money into his account. This was an attempt to engage the reciprocity principle by giving the victim the impression that a great favour had been done for him. By doing so, the victim became compelled to return the favour in terms of giving greater trust to the scammer as well as giving the scammer a substantial amount of his own money when she appeared in need.

"...put in her own money, her 200,000, into my account. ... She said she didn't have any money, so I lent her some money, I lent her like another 500,000, all right, to help her out. So I liquidated some of my big positions and to help her out, she said she'll pay me back, you know, because I thought I trusted this woman."

"She's a fashion designer ... doing something called cheongsam fashion designs for fashion house. ... She started talking about food and she started talking about things like great places to eat in Hong Kong. ... Then she introduced me to this gold thing..."

The case study also reflects the relationship building element of pig-butchering scams, which abuses the liking principle. In this case, the scammer claimed to be someone who worked in the fashion industry and started building rapport with the victim by engaging him in extended conversation. The scammer introduced the victim to a gold investment and convinced him to invest in it only after engaging in the relationship building process for some time. This seems to be the unique pig-butchering characteristic of building a relationship with the victim and grooming them through conversation, before introducing a fraudulent investment vehicle once enough trust and liking has been gained.

"She thought I had great potential..."

The scammer further utilised liking to their advantage by claiming the victim had the capacity to do much more with the investment. This likely made the victim feel like he was recognised and in turn made him more willing to listen to the scammer as he saw them more positively in return.

The victim was also pressurised when the scammer told him about the extreme measures taken by investors to pay the fees that were asked of them – planting the idea that people take drastic measures when attempting to get the promised returns. This might have made the victim take actions beyond what he previously thought reasonable in order to pay the fees, as his only point of comparison was the scammer.

> **"She sold some of her jewellery, she sold her car, she borrowed some money from her parents..."**

The investment scam creates the ideal conditions for sunk cost to take effect. In this case, the victim was told to pay for many strange fees and ended up having to liquidate a significant part of their assets to afford them. The initial fee is a critical element as it commits the victim to the investment scam since they now have a stake in it, making them unwilling to disengage from the fraudulent investment.

> **"...8% for risk management because you made too much money. ... so I had to find 400,000, so I had to liquidate some stuff. And uh, all my assets, all my shares..."**

> **"When you're in too deep, you just want to get out and you just can't accept that you've been scammed."**

A particularly important confession by the victim was that he found it extremely difficult to accept that he had been scammed once he had lost too much. This suggests that sunk cost is a very powerful cognitive bias in investment scams due to the amount of money progressively lost through the process, which makes it more and more difficult for the victim to disengage from the scam as they want to believe that they can get their money back somehow. Confirmation bias exacerbates this effect, as victims so desperately want to believe that the investment product is real that they end up ignoring all the disconfirming evidence that they have in fact been caught in an investment scam.

Another important characteristic of investment scams surfaced by the case study is the attempt to lull victim into a false sense of security by making him think he has control. After some initial earnings, the victim was initially allowed to withdraw some of his money. This shows how scams are evolving to give victims the illusion that they can get their money back anytime, which encourages them to invest even more money and leads to even greater losses in the long run. This false sense of control may cause victims to possess a misguided confidence in the legitimacy of the investment, causing them to miss other signs that something is amiss.

> **"...then she suggests me to withdraw. So I actually made two successful withdrawals through the website, okay..."**

Psychological Frameworks

This case study supports some of the psychological models explored in this paper. The thought process of the victim in this case reflects some predictions of Construal Level Theory. The victim agreed that he did have an abstract idea that he wanted to use the profits he would gain from the investment to retire earlier. As Construal Level Theory states, when the mental construal is more psychologically distant, it also becomes more abstract and specific details relevant to concepts like feasibility are given less weight. As a result, the victim decides to invest because they are fixated on the idea of being able to retire earlier in the long run and miss the flaws in the claims of the investment scam.

> **"...an abstract idea in mind ... I really wanted to make this money... retire early..."**

The victim also mentioned being excited when he was engaging with the investment scam opportunities. Using the Elaboration Likelihood Model, it is possible that due to lacking the ability to carefully deliberate as a result of the heighted emotions

> **"It was exciting, I was excited, right."**

from his excited state, he used a more peripheral route. This ultimately caused him to fail to identify the issue with the investment scam.

Psychosocial Variables

"I got greedy, I mean, I thought I could retire..."

There are certain psychosocial variables of interest that were brought up during the interview. For example, the victim often identified his mistakes as being the result of greed. This is supported by research suggesting that traits such as materialism can make individuals more vulnerable to investment scams. In essence, the pursuit of material gains may dull an individual's ability to detect when they are caught in a scam. Although this is likely to prove to be difficult, it is important to consider how we can encourage the public to take a step back and re-evaluate the situation when they find themselves propelled by monetary incentives.

"I'm a very friendly person..."

The victim also noted that he considered himself to be a friendly individual before the scam occurred, suggesting that the personality trait of agreeableness may be a risk factor, possibly because agreeable people are more inclined to do as others ask.

Social Isolation

"she told me not to tell anyone..."

It is worth noting that the scammer told the victim to avoid informing anyone else about what was going on. This reveals a very intentional attempt to isolate the victim from support networks that could detect the scam, suggesting that scammers themselves are aware of the power of an external perspective and actively take countermeasures against it. In turn, this suggests that attempts to encourage people to look out for their friends and family can prove effective if they know the warning signs to look out for.

Investment Scam Effects

The effects of investment scams are important to explore as well. Similar to findings in the research, the victim in this case reported being in a state of depression and feeling that there was nothing he could possibly do, especially when confronted with the thought of having to return all the money he borrowed for the investment. It is evident that the psychological impact of investment scams is highly damaging, potentially ingraining a sense of helplessness and feeling of being overwhelmed in victims.

"There's no way in the world I can do anything. So I was very, very depressed at that stage, right, and then I just stop paying it and then I realise I've got to pay all these loans now, right?"

Investment Scam Red Flags

"... this person had a winning rate of literally 9 out of 10 trades. 9 out of 10, well that's just unheard of..."

This interview was also able to provide some insights into potential red flags that the public should be aware of. Firstly, the victim noted that the rate at which the scammer seemed to make money off the investment was unbelievable compared to what is generally expected. When investment products seem to produce returns that are unbelievable, individuals should be highly suspicious and investigate the validity of the product as the results are likely faked.

"the red flag would be if the person does not do a video call, in person with you ... red flag is if there is no local contact number..."

Beyond this, a refusal to video call for identity verification is a sign of a potential scam, as scammers tend to utilise fake profiles and are hence unable to do any kind of video calling. The use of a foreign number and lack of a local number is another indicator, as investment scam syndicates tend to be based overseas and hence must contact victims using a foreign number.

Finally, the demand for fees in return for being able to withdraw money is a significant indicator that the investment product is likely a scam, as scammers use this to try to get victims to pay exorbitant fees in order to release the money they have supposedly earned, although they have no intention of returning victims anything at all.

> **"I think that's the red flag, right, if they demand for more money to withdraw money, then that's pretty much you'll never get your money back kind of thing".**

IMPLICATIONS FOR CRIME PREVENTION

The extensive literature review, supplemented by the case study analysis, provide some insights into how to enhance crime prevention against investment scams. However, it is worth noting that the implications outlined here stem primarily from insights gleaned through comprehensive literature review, which lay the foundation for comprehending the phenomenon of investment scams. The accompanying case study contributes depth and specificity, enhancing our understanding of the pig-butchering variant within the context of Singapore. With that in mind, the potential implications for crime prevention are as outlined below.

Firstly, Construal Level Theory suggests that it is important to encourage people to be especially attentive to finer details if they are being offered an investment product that is built for the long term. Due to the psychological distance, people may be inclined to focus more on the big picture and the desirability of the potential returns instead of feasibility. However, it is precisely in this situation that the public must ensure they understand the specific details of how the investment scheme works, to verify they will really obtain what they want from the investment.

Secondly, the Elaboration Likelihood Model informs us that scammers are likely to abuse the vulnerability of the peripheral route. Hence, it is important to educate the public on common cognitive biases and persuasion techniques, to improve their chances of identifying them and staying on guard. When the public is better able to identify the tactics used by the scammers, the suspicion that arises when similar tactics are used on them should help to prevent the peripheral route from being activated easily.

Thirdly, it is important to recognise that the new wave of investment scams may allow victims to withdraw money at the start to make them less cautious. Hence, the public should be warned that they should remain vigilant despite successful, initial withdrawals. It is necessary to continue to check on the legitimacy of the investment scheme throughout the process.

Lastly, there are certain scam indicators that the public should be made aware of regarding investment scams. This includes indicators such as an attempt to isolate the victim, a refusal to video call and the charging of exorbitantly high fees for withdrawal of money. Recognising these indicators can improve the public's ability to identify an investment scam. Hence, SPF has collaborated with the National Crime Prevention Council to curate anti-scam campaign posters that are specific to scam types (e.g., investment scam) and disseminate them both physically (e.g., in lifts, at bus stops) and online (e.g., ScamAlert website) with the aim of raising public awareness of these indicators of interest.

LIMITATIONS AND FUTURE STUDY

Notwithstanding the rich insights provided by the case study approach, there are some limitations in this study that are worth noting. Firstly, case study approach, particularly the use of a single case study, provides little basis for generalisability of findings (Yin, 2014). However, this is not the primary aim of this study. Rather, the study aims to gain in-depth insights and particularised knowledge essential for enriching one's understanding of pig-butchering scams, which is integral for tailoring crime prevention efforts effectively. Furthermore, the case study approach lends itself well in providing insights into such explanatory 'what' (e.g., what are the psychological processes and persuasion techniques involved?) and 'how' (e.g., how can we prevent it?) questions (Crowe et al., 2011).

Nevertheless, future studies could build upon this study by taking a multiple case studies approach to enhance external validity or conduct quantitative analysis on victim statements of facts to validate the robustness of these findings. Secondly, there may be potential concerns regarding construct validity due to two primary factors: i) the predominant reliance on a sole coder (i.e., first author) which may introduce researcher subjectivity (Idowu, 2016; Takahashi & Araujo 2020); and ii) the exclusive reliance on the victim interview as the only source of information. Future studies could involve multiple coders to ensure inter-rater reliability and minimise researcher subjectivity, as well as employing data triangulation using multiple sources of information to verify the reliability of interpretations (Stake, 2003).

CONCLUSION

In conclusion, this study sheds light on various critical aspects of investment scams, particularly victim characteristics, persuasion techniques, cognitive biases, psychosocial variables, psychological frameworks, and potential red flags/indicators. The examination of persuasion tactics, such as the abuse of authority and reciprocity principles, elucidates how scammers exploit psychological vulnerabilities to manipulate victims. On the flip side, insights into cognitive biases like sunk cost and confirmation bias underscore the challenges victims encounter in disengaging from scams. Similarly, the discussion on psychosocial variables highlights the role of traits like materialism and agreeableness in influencing victims' vulnerability to scams. Additionally, the exploration of psychological frameworks, such as Construal Level Theory and the Elaboration Likelihood Model, offers valuable insights into victims' decision-making processes and susceptibility to scams.

Lastly, the identification of red flags – such as unrealistic returns, refusal of identity verification, and constant demands for fees – provides practical guidance for detecting potential scams. All these underscore the multidimensional nature of investment scams and the imperative for holistic prevention and intervention strategies informed by psychological insights and empirical evidence. Although this study is mainly exploratory, it can serve as a foundation for more comprehensive future research in this area to intricately examine the psychological mechanisms involved in different types of pig-butchering scams and their impacts on victims involved. More importantly, the recommendations outlined remain valuable in effectively safeguarding the public against pig-butchering scams, potentially one of the most financially detrimental scam variants in Singapore presently.

ABOUT THE AUTHORS

Low Eu Hian
is a final year Psychology student from Singapore Management University. During his internship at Police Psychological Services Department of the Singapore Police Force, he investigated trends in domestic homicide cases through case coding and analysis. He further embarked on research into the factors underlying psychological vulnerability to scams. He has a keen interest in forensic and clinical psychology.

Tan Wei Liang
is a psychologist with the Operations and Forensic Psychology Division of the Police Psychological Services Department. He has a broad interest in crime and psycholegal research, specialising in scam-related research as part of his job. Additionally, he trains law enforcement officers on investigative interviewing, victim support, and police intelligence, as well as assists in profiling work.

Carolyn Misir
is a principal psychologist in the Operations and Forensic Psychology Branch (OFP) of the Police Psychological Services Department, which supports police operations, crime investigations, victim support and police intelligence through offence research and profiling projects as well as direct consultations with units in high profile on-going cases. Carolyn oversees the crime research areas of the work in OFP while building deep domain expertise and research in the areas of investigative, victim and criminal psychology. Carolyn has a concurrent appointment at Home Team Psychology Division as a principal psychologist within the Forensic Expert track.

Associate Professor Dr Jansen Ang
is a Senior Principal Psychologist with the Ministry of Home Affairs in Singapore. Trained as a Forensic Psychologist at the University of Surrey in the United Kingdom, he holds various appointments within the Home Team. At Ministry Headquarters, he is the Deputy Chief Psychologist responsible for Crisis Operations and Research of the psychologists serving in the Police, Narcotics, Civil Defence, Prisons, Immigration and Checkpoints Authority and the Home Team Academy. He is also responsible for the Home Team's psychological response in times of national crises and disasters as well as the coordination of psychological research to support Home Team needs. Additionally, he oversees the deployment of the Human Emergency Assistance Response Team (HEART). In the Singapore Police Force, he is the Director of the Police Psychological Services Department (PPSD) which provides psychological services to police officers, police operations and investigations as well as supports organizational excellence in the police. He is also the Police's representative on the National CARE Management Committee that is a national body responsible for managing the psychological impact arising from national crises and incidents. He also teaches at the Nanyang Technological University in the College of Humanities and Social Sciences. Jansen's current research interests are in the area of organised crime profiling as well as the development of services to support law enforcement officers and operations.

REFERENCES

Ajzen, I. (1991). The theory of planned behavior. *Organizational Behavior and Human Decision Processes, 50*(2), 179–211. https://doi.org/10.1016/0749-5978(91)90020-T

Anti-Deception Coordination Centre. (2023, June). *Scam Statistics | Anti-Deception Coordination Centre(ADCC) | Hong Kong Police Force*. https://www.adcc.gov.hk/en-hk/statistic.html

Arkes, H. R., & Blumer, C. (1985). The psychology of sunk cost. *Organizational Behavior and Human Decision Processes, 35*(1), 124–140. https://doi.org/10.1016/0749-5978(85)90049-4

Bailey, J., Kingston, P., Taylor, L., & Eost-Telling, L. (2019). THE HEALTH IMPACT OF SCAMS. *Innovation in Aging*, 3(Supplement_1), S757–S757. https://doi.org/10.1093/geroni/igz038.2781

Chuang, J.-Y. (2021). Romance Scams: Romantic Imagery and Transcranial Direct Current Stimulation. *Frontiers in Psychiatry, 12*, 738874–738874. https://doi.org/10.3389/fpsyt.2021.738874

Cialdini, R. B. (2007). *Influence: The psychology of persuasion.* (EPub edition.). HarperCollins Publishers.

Crowe, S., Cresswell, K., Robertson, A., Huby, G., Avery, A., & Sheikh, A. (2011). The case study approach. BMC Med Res Methodol, 11, 100. https://doi.org/10.1186/1471-2288-11-100

Deliema, M., Shadel, D., & Pak, K. (2020). Profiling Victims of Investment Fraud: Mindsets and Risky Behaviors. *The Journal of Consumer Research, 46*(5), 904–914. https://doi.org/10.1093/jcr/ucz020

Faux, Zeke. (2024, February 29). New Study Estimates as Much as $75 Billion in Global Victims' Losses to Pig-Butchering Scam. *Time*. https://time.com/6836703/pig-butchering-scam-victim-loss-money-study-crypto/

Federal Bureau of Investigation. (2022). *Internet Crime Complaint Center(IC3) 202*1 | Annual Reports. https://www.ic3.gov/Home/AnnualReports

Habib, R., & Dixon, M. R. (2010). NEUROBEHAVIORAL EVIDENCE FOR THE "NEAR-MISS" EFFECT IN PATHOLOGICAL GAMBLERS. *Journal of the Experimental Analysis of Behavior, 93*(3), 313–328. https://doi.org/10.1901/jeab.2010.93-313

Hidajat, T., Primiana, I., Rahman, S., & Febrian, E. (2020). Why are people trapped in Ponzi and pyramid schemes? *Journal of Financial Crime, 28*(1), 187–203. https://doi.org/10.1108/JFC-05-2020-0093

Idowu, O. E. (2016). Criticisms, Constraints and Constructions of Case Study Research Strategy. *Asian Journal of Business and Management, 4*(5), 184–188.

Kadoya, Y., Khan, M. S. R., & Yamane, T. (2020). The rising phenomenon of financial scams: Evidence from Japan. *Journal of Financial Crime, 27*(2), 387–396. https://doi.org/10.1108/JFC-05-2019-0057

Liberman, N., & Trope, Y. (1998). The role of feasibility and desirability considerations in near and distant future decisions: A test of temporal construal theory. *Journal of Personality and Social Psychology, 75*(1), 5–18. https://doi.org/10.1037/0022-3514.75.1.5

National Crime Prevention Council. (2023). *Stories*. Default. https://www.scamalert.sg/stories

Nguyen, N. T., Nguyen, A. T., To, H. T. N., & Le, T. T. H. (2023). Why are Vietnamese people susceptible to cryptocurrency Ponzi schemes? Findings from using the PLS-SEM approach. *Journal of Financial Crime, 31*(1), 158–173. https://doi.org/10.1108/JFC-12-2022-0299

Nickerson, R. S. (1998). Confirmation Bias: A Ubiquitous Phenomenon in Many Guises. *Review of General Psychology, 2*(2), 175–220. https://doi.org/10.1037/1089-2680.2.2.175

North American Securities Administrators Association. (2023). Top Investor Threats. *NASAA*. https://www.nasaa.org/investor-education/fraud-center/top-investor-threats/

Onay, S., La-ornual, D., & Öncüler, A. (2013). The Effect of Temporal Distance on Attitudes toward Imprecise Probabilities and Imprecise Outcomes. *Journal of Behavioral Decision Making, 26*(4), 362–374. https://doi.org/10.1002/bdm.1763

Oskamp, S. (1965). Overconfidence in case-study judgments. *Journal of Consulting Psychology, 29*, 261–265. https://doi.org/10.1037/h0022125

Petty, R. E., & Cacioppo, J. T. (1986). *Communication and Persuasion*. Springer. https://doi.org/10.1007/978-1-4612-4964-1

Pressman, S. (1998). On Financial Frauds and Their Causes. *The American Journal of Economics and Sociology, 57*(4), 405–421. https://doi.org/10.1111/j.1536-7150.1998.tb03373.x

Rebane, T., & Watson, I. (2024, June 20). Killed by a scam: A father took his life after losing his savings to international criminal gangs. He's not the only one. *CNN*. https://edition.cnn.com/2024/06/17/asia/pig-butchering-scam-southeast-asia-dst-intl-hnk/index.html#:~:text=According%20to%20FBI%20data%2C%20out,stolen%20in%20pig%20butchering%20scams.

Singapore Police Force. (2024, February). *Annual Scams and Cybercrime Brief 2023*. Singapore Police Force. http://www.police.gov.sg/Media-Room/Statistics

Stake, R. E. (2003). Case studies. In N. K., Denzin, & Y. S., Lincoln (Eds.), *Strategies of Qualitative Inquiry* (2nd ed., pp. 134–164). Sage Publications.

Takahashi, A. R. W., & Araujo, L. (2020). Case study research: opening up research opportunities. *RAUSP Management Journal, 55*(1), 100–111. https://doi.org/10.1108/RAUSP-05-2019-0109

Thaler, R. H., & Johnson, E. J. (1990). Gambling with the House Money and Trying to Break Even: The Effects of Prior Outcomes on Risky Choice. *Management Science, 36*(6), 643–660. https://doi.org/10.1287/mnsc.36.6.643

Trope, Y., & Liberman, N. (2010). Construal-level theory of psychological distance. *Psychological Review, 117*(2), 440–463. https://doi.org/10.1037/a0018963

Vu, P. & Feinstein, S. (2017). An exploratory multiple case study about using game-based learning in STEM classrooms. International *Journal of Research in Education and Science (IJRES), 3*(2), 582-588. https://doi.org/10.21890/ijres.328087

Wang, F., & Zhou, X. (2023). Persuasive Schemes for Financial Exploitation in Online Romance Scam: An Anatomy on Sha Zhu Pan (□□□) in China. *Victims & Offenders, 18*(5), 915–942. https://doi.org/10.1080/15564886.2022.2051109

Weinstein, N. D. (1980). Unrealistic optimism about future life events. J*ournal of Personality and Social Psychology, 39*(5), 806–820. https://doi.org/10.1037/0022-3514.39.5.806

Wen, X., Xu, L., Wang, J., Gao, Y., Shi, J., Zhao, K., Tao, F., & Qian, X. (2022). Mental States: A Key Point in Scam Compliance and Warning Compliance in Real Life. International *Journal of Environmental Research and Public Health, 19*(14), 8294. https://doi.org/10.3390/ijerph19148294

Whitty, M. T. (2020). Is There a Scam for Everyone? Psychologically Profiling Cyberscam Victims. *European Journal on Criminal Policy and Research, 26*(3), 399–409. https://doi.org/10.1007/s10610-020-09458-z

Yin, R. K. (2014). *Case Study Research: Design and Methods*. Sage.

HOW ARE NATIONAL SECRETS LEAKED?
AN ANALYTICAL STUDY

Vappala Balachandran
Independent Researcher
Former Special Secretary, Cabinet Secretariat of the Government of India

ABSTRACT

There are many reasons why intelligence leaks take place, ranging from the infiltration of government organs by hostile powers, local activist groups, and independent media seeking transparency, to the emergence of self-motivated home spies driven by ideology or pecuniary gain. This article, written by a former deputy head of the Indian intelligence service, also examines the impact of faulty government procedures post-9/11 and the challenges posed by outdated electronic communications systems in the era of rapid technological advancement, including the advent of Artificial Intelligence. Additionally, it highlights the dangerous tendency of certain governmental wings to conduct secret state to state negotiations without following necessary security precautions when they should have used their secret channels of intelligence services for such sensitive negotiations.

LEAKING INTELLIGENCE

Experience tells us that national secrets are leaked in the following situations:

1. Penetration of government organs by hostile or friendly powers for clandestine intelligence extraction.
2. Self-motivated home based spies who, for ideology, religion, or pecuniary reasons, work for foreign agencies.
3. Leaks to local activist groups or non-government organisations (NGOs) to press for the Right of Information and demand more accountability from the government; or to the free media wanting more transparency in government decision making, including the security sector.
4. Flaws in the procedures established by governments after the 9/11 attacks for speedier dissemination of intelligence to operational groups for quick counter-terrorist operations.
5. Difficulty in implementing security instructions in the new ecosystem when existing electronic communications systems are getting rapidly outdated by new inventions like Artificial Intelligence (AI).
6. Tendency of the leadership of some government agencies to assume responsibility over secret state to state negotiations without following necessary security precautions or when they use secret documents for political purposes.

Although most attention is focused on government leaks, it should be noted that hostile powers target not only governments, but also private enterprises which are increasingly assuming responsibility for operating in the critical information technology and intellectual property sectors – industries that form the core strength of any country's national security.

1. PENETRATION BY HOSTILE OR FRIENDLY POWERS

History is full of cases of espionage carried out by both hostile and 'friendly' nations. Indeed, there is an unwritten axiom in the intelligence world that sources should be planted when bilateral relations become friendly. In the 1980s, for instance, French intelligence agents broke into the Indian Prime Minister's office using the "Coomar Narain spy syndicate" even while India was in the process of purchasing defence equipment including fighter planes from France. Intelligence agencies have a special task of obtainting secrets for their governments which other government departments cannot. Political masters do not care how it is done; the key is to not get caught (Balachandran, 2014).

Similarly, when European leaders proclaimed themselves to be "shocked" when European newspapers reported in May 2021 that Denmark had helped the US spy on Germany, France and other European allies between 2012 and 2014, the US Politico news portal carried a commentary titled "Spying on allies is normal. Also smart." As columnist Elizabeth Braw noted, "nations don't have friends, a famous French leader once said, only interests. And spying among even close allies is not only common practice – it's very often a good idea" (Braw, 2021).

Some diplomatic fallout can, however, be expected when friends are caught spying on each other, although the damage is rarely permanent. When Edward Snowden leaked a trove of documents in 2013 that exposed US spying operations around the world, the reaction from allied governments was swift but designed more to dampen public anger: The CIA station chief in Berlin was expelled and (later quietly replaced); the American ambassador in Paris was summoned for a dressing-down.

Adversarial spying is, however, framed as a serious threat to national security, a good example being the combined "Five Eyes" alliance charge against China. On October 23, 2023, the directors of the security intelligence agencies of of the so-called "Five Eyes" alliance – Christopher Wray of the US Federal Bureau of Intelligence, Mike Burgess of the Australian Security Intelligence Organisation, David Vigneault of the Canadian Security Intelligence Service, Ken McCallum of the United Kingdom MI5 and Andrew Hampton of New Zealand Security Intelligence Service – gave an unprecedented joint interview to an American TV network where they left no doubt they believed China to be "the greatest espionage threat democracy has ever faced" (Pelley, 2023).

Wray had begun to sound the alarm in July 2020 when he gave a public lecture detailing the US intelligence community's assessment of the threat posed by the Chinese government to American national and economic security. This was perhaps the first time any nation has been so specifically blamed for massive intelligence operations against another country after the end of the Cold War.

In his 2020 speech, Wray said that he was giving more details on the Chinese threat "than the FBI has ever presented in an open forum" in view of its importance. The Chinese government and the Chinese Communist Party had been adopting "a diverse and multi-layered policy" which included economic espionage, cyber intrusions, clandestine efforts, threats to academia, exercising malign foreign influence, and breaking the rule of law by exploiting America's openness in business and information sectors (Wray, 2020).

The FBI believed, Wray said, that the Chinese were stealing personal data to achieve its goal of becoming the world leader in artificial intelligence (AI) as this type of data "feed right into China's development of artificial intelligence tools". Another reason would be to locate and identify persons who had access to the American government's sensitive information and then motivate such people to try to steal it for them.

During the past decade, the FBI had seen economic espionage cases involving China surging by 1,300%. Several cases investigated by the FBI suggested that academics of Chinese origin were being motivated to subscribe to the Chinese policy of "Thousand Talents Programme" and to entice them to secretly bring American "knowledge and innovation back to China" even if it meant stealing proprietary information or violating American export controls.

American companies seeking access to Chinese partners and markets have also been subject to "malign foreign influence", Wray said, adding: "If China's more direct, overt influence campaign doesn't do the trick, they sometimes turn to indirect, covert, deceptive influence efforts" (Wray, 2020).

A Washington DC think tank, the Center for Strategic & International Studies, recently published a survey of Chinese espionage cases in the US since 2000, and concluded that the 224 cases of Chinese espionage it compiled based on publicly available information "far outnumber any other country, even Russia" (Center for Strategic and International Studies, n.d.).

China rejected the charges on 23 October 2023 by calling the Five Eyes intelligence alliance a "security threat " to our countries because of its "Cold War mentality and ideological bias" (Aktaş, 2023). A more detailed denial appeared months later, through an editorial by *Global Times* on March 26, 2024, after the UK government accused China of being

behind a string of cyberattacks on British politicians. *Global Times*, which bills itself as "China's most informative English-language newspaper" accused The Five Eyes alliance of being "the world's largest intelligence organization, with the 'big brother' US being the world's largest 'hacker empire'." It reminded the world that four years ago China had proposed a "global initiative on data security" to prevent using information technology to undermine critical infrastructure. Quoting the Chinese foreign ministry spokesman, the paper added: "If 'the Five Eyes alliance' truly wants to keep cyberspace safe, they are welcome to join the Global Initiative on Data Security" (Global Times, 2024).

Intelligence historians have often found it difficult to compare the proportionate damage to home national security by 'friendly' or 'adversarial' spying. It is often said that 'friendly' spying is more perilous for the target country as it catches the foreign, home or defence ministries off their guard, unless their counter-intelligence agencies are hypervigilant. Adversarial spying, on the other hand, is more anticipated.

Is a free society more vulnerable to being targeted than authoritarian nations? Here we must listen to what Polish spy Pawel Monat, who defected to the US after a successful innings in US as military attache, had to say in his 1962 book *Spy in the US* which he wrote jointly with John Dille, then military editor of *Life* magazine: "America is a delightful country to carry out espionage … one of the weakest links in the national ssecurity is the yearning friendliness of her people" (Monat & Dille, 1962).

Who has the edge in the current technical intelligence war between the West and China? On 15 May 2024, the BBC's security correspondent Gordon Corera reported that the West is "struggling" to keep pace with the Chinese threat assisted by a resurgent Russia. Citing interviews with current and former spy chiefs in the UK and Australia, Corera wrote that the Western agencies failed to realise this threat till recently and "has fallen behind in intelligence terms, leaving the West more vulnerable to Beijing's spying, and both sides at risk of a potentially catastrophic miscalculation". He also quoted a Western intelligence official as estimating that China employs around 600,000 people on intelligence and security, "more than any other state in the world" (Corera, 2024).

2. SELF-MOTIVATED HOME SPIES

The motivation for home spies willing to work for hostile or friendly nations differ from case to case. In brief, it could be summarised as "Money, Ideology, Coercion and Ego"(MICE). Religion could be a fifth motivation, but not always. Allen Dulles says in *The Craft of Intelligence* that the Soviets always used "love, sex and greed" as "weapons to ensnare people" to work for them. He adds another category of "intelligence swindler" who goes from embassy to embassy trying to "sell" intelligence. Any trained intelligence officer could spot such "cranks and crackspots". I shall try to deal with these cases as follows:

Ideology

British diplomats David Maclean and Guy Burgess, intelligence officer Harold "Kim" Philby, art historian Anthony Blunt and British civil servant John Cairncross were known as "**The Cambridge Five**" since they were all recruited on ideological affinity while at Cambridge University in the 1930s. The Five believed that Communism was the best bulwark against the rising fascism in Europe. They attracted attention being from the elite class and having held high positions in government and society. What infuriated the public and media was the way successive governments in Britain handled this worst security scandal by not divulging the details to the public. In the absence of any official statements, the public believed exaggerated media stories that their entire government system was complicit in the suppression of information and that it was totally penetrated by the Soviet Union. Of the Five, David Maclean, Guy Burgess and Kim Philby died in Moscow. Blunt was granted full immunity from prosecution by MI5, which also decided to keep the whole matter under wraps for 15 years in return for his full confession in 1964. However, he was stripped of all honours like knighthood and Honorary Fellowship of Trinity College. Blunt, in turn, revealed the fifth man, John Cairncross, to MI5 in 1964 itself.

Another person who spied for ideological considerations was American Defence Intelligence operative **Ana Montes** who was arrested by the FBI in 2001 on charges of spying for Cuba. She was sentenced in 2002 to 25 years in prison but released after 20 years in 2023 for good conduct (Balachandran, 2023).

The arrest of Ana Montes led to another discovery of "one of the highest-reaching and longest-lasting infiltrations of the US government by a foreign agent" as described by US Attorney General Merrick Garland in December 2023 while arraigning **Victor Manuel Rocha**, former US ambassador to Bolivia, for spying for Cuba for four decades. Rocha, who was born in Colombia, became a naturalised US citizen in 1978 and occupied high level positions in the US State Department including adviser to the commander of the US Southern Command, whose area of responsibility included Cuba (Yilek, 2024). It is said that Rocha's motivation to work as a spy was " ego, grudge and resentment" since he never "felt accepted among the US establishment elite" (Tait, 2023).

However, Ana Montes and Rocha never contacted each other, and played their games by strictly following the spy tradecraft of restrictive security. It was an old CIA operative named Felix Rodriguez who took part in the infamous 1961 "Bay of Pigs" operation, who got the first clue of their espionage in 2006 from a defecting Cuban army officer (Goodman & Mustian, 2024).

Patriotism

The earliest case in history of somone spying for patriotic reasons is a Greek businessman named **Demartus**, recorded by Herodotus (484-425 BCE), "the father of history". Demartus witnessed the military build-up by Xerxes against Athens and Sparta and decided to inform his home country. He used "steganography" (secret writing) for the first time in history. In Greek, "*steganos*" means "covered" and "*graphien*" means "to write". Demartus used a very innovative method to convey this advance intelligence. He used wooden folding tablets, which he was exporting to Greece, as the medium. He scraped the wax off a pair of tablets, wrote his message conveying details of military build-up by Xerxes, applied wax over it and sent the consignment to Greece. In that way, the Persian guards or customs officials could not detect the secret message (Balachandran, 2022).

Jonathan Jay Pollard, a US Naval Investigative Service analyst who spied for Israel during 1984-85 is considered Israel's national hero. He pleaded guilty in 1987 to handing over ten volumes of US signals intelligence folders to his handler and was given a life term in prison. On 7 January 2008, the Jerusalem City Council renamed their "Paris Square" outside the US Consulate and the Prime Minister's house as "Freedom for Jonathan Pollard Square".

Religion

The American Office of Strategic Services, the precursor of the CIA, reportedly used to recruit missionaries because they were some of the best clandestine operatives. The missionaries might not have been recruited on religious grounds, but their vocation gave them useful skillsets. According to Matthew Sutton, author of *Double Crossed: The missionaries who spied for the United States during the Second World War*: "Missionaries have excellent language skills, they understood cultural sensibilities, they knew how to disappear into foreign cultures, and they were masters at effecting change abroad. By the end of the war, American missionaries were gathering intelligence, keeping tabs on Axis agents, drafting plans to infiltrate enemy territory, and partnering with insurgent groups." (Foster, 2020).

Pecuniary reasons

The majority of spies belong to this category. Some well-known cases include Coomer Narain of India, who "startled a court today by confessing that he sold vital national secrets for over 25 years to France and another Western nation and had made $1 million as a spy" (*Los Angeles Times*, 4 February 1985); US Navy radioman John Anthony Walker, who caused the US Navy's "biggest betrayal" in the 1960s by providing "Moscow access to weapons and sensor data and naval tactics"; Edward Lee Howard of the CIA, who defected to the Soviet Union in 1985; Aldrich Ames, a top CIA officer who exposed many CIA assets to Moscow in the 1990s; FBI agent Robert Philip Hanssen who divulged FBI surveillance operations to the Soviets in the same era (Balachandran, 2022).

3. LEAKS TO ACTIVISTS OR MEDIA

Most governments have laws that punish the leaking of classified information and those who break them risk prosecution. In a democracy, however, the leaking of government secrets might not be considered a national danger as the intention of the civil society is for the public good – to demand more transparency. As a 2021 Carnegie Endowment

paper examining the pandemic period has observed, such actions by civil society are "on their own out of frustration at governments' sluggish and inadequate responses to the emergency". A similar opinion was put forward by World Health Organization (WHO) in 2023 that civil society organisations "can reinforce transparency, monitoring, public trust, and programme delivery through uncorrupted resource mobilisation mechanism".

However, there have been reports that some civil society organisations were punished by their governments during the COVID-19 period for demanding more transparency. Rustagi & Wu (2020) have documented some cases from India.

In October 2021, the International Consortium of Investigative Journalists (ICIJ) reported that scribes in some countries like Honduras, Russia, Ecuador, Republic of Congo, Serbia, Colombia, Belarus, Pakistan, Turkey, and Hong Kong, who exposed the "Pandora Papers" (11.9 million documents containing secret offshore bank account details of 35 world leaders) were penalised by their local authorities for revealing that these leaders had stashed away between US$5.6 to 32 trillion.

Some media organisations have sought to justify the publishing of government secrets. On 1 July 2006, *New York Times* published an unusual joint op-ed by the editors of New York Times and *Los Angeles Times* titled "Why Do We Publish a Secret?" They began by quoting the 1971 US Supreme Court ruling by Justice Hugo Black refusing to suppress the publication of a secret government history of the Vietnam War: "The government's power to censor the press was abolished so that the press would remain forever free to censure the government. The press was protected so that it could bare the secrets of the government and inform the people" (Baquet & Keller, 2006).

The two newspapers justified their editorial decisions to publish secrets by assuring the readers that they always carefully weighed "the merits of publishing against the risks of publishing" by scrutinising the contents of each report to ensure that no operational information was revealed. They also gave opportunities to the concerned government agencies to raise objections, and cited three examples where reports were withheld because they would have jeopardised national security. These were on nuclear stockpiles, a sensitive counter-terrorist action, and the discovery of American espionage activities in Afghanistan.

They concluded their joint op-ed with these remarks: "We understand that honorable people may disagree with any of these choices – to publish or not to publish. But making those decisions is the responsibility that falls to editors, a corollary to the great gift of our independence. It is not a responsibility we take lightly. And it is not one we can surrender to the government."

Not all governments accept this argument. In September 2023, French internal security officials searched the home of *Disclose* correspondent Ariane Lavrilleux at dawn and took her into custody for publishing hundreds of papers "that alleged French intelligence was used to target civilians in Egypt" (*The Guardian*, 19 September 2023). *Disclose*, a French investigative website created in 2018 on the lines of the American *ProPublica* and the German *Corrective*, has been quoting from classified French government documents since its first investigative report on 15 April 2019. According to *The Guardian*: "The *Disclose* articles [written by Lavrilleux] said the leaked documents showed the information from French intelligence was used in at least 19 bombings against smugglers in the region between 2016 and 2018. The documents also showed officials within the French government had warned that the Egyptian state could use the information from the counter-intelligence operation codenamed Sirli, but the operation was allowed to continue."

4. FAULTY PROCEDURES

Prior to the 9/11 attack, the CIA and FBI worked in silos and did not share information, resulting in the biggest calamity in recent US history. This was severely criticised by the 9/11 National Commission. Like in all democratic bureaucracies, the pendulum swung into the opposite direction: from a rigorously restrictive circulation of intelligence reports to more widespread dissemination.

In America, security clearance is given to individuals even after changing jobs, especially if they work for private defence contractors. Periodical reviews are done: "Top Secret" label will be reviewed after 5 years, "Secret" after 10 years and "Confidential"

after 15 years. This is, however, not a totally reliable system. As against this, in India, for example, the day an employee changes a security job, the security clearance stops. If he/she is employed in another security job, a fresh security clearance must be given.

The US system has been criminally misused by junior level defence-intelligence employees – Jack Teixeira (21), Chelsea Elizabeth Manning (23), Edward Snowden (24) and Reality Leigh Winner (25).

(a) **Jack Teixeira**, the "Ukraine war intelligence leaker", was only a National Guardsman, a comparatively low rank. He joined the US Air National Guard in Massachusetts in 2019, and because the Air National Guard is responsible for the US Air Force's tactical airlift support and combat communications with total responsibility for air defence of the entire country, he was accorded Top Secret and "sensitive compartmented information" clearance. US National Guards (Army and Air) are federal reserve forces, which during peacetime work under the governor of each state. Teixeira did not appear to have had any intentions of betraying his country; reports suggest he was "showing off" his leadership qualities by posting important news on Discord, a social media messaging site popular with "gamers". He wanted his friends to recognise him as "OG", their de facto leader.

(b) **Chelsea Elizabeth Manning**, the "Wikileaks" leaker who released more than 700,000 classified documents in 2010 as a "form of protest" against American wars in the Middle East, joined the army in 2007 at the age of 20. She was physically small, just five feet high and could not stand bullying by her peers. She also had a disturbed childhood due to gender dysphoria and parental alienation. She took advantage of her "Top Secret-Sensitive Compartmentalised Security" (TSSCS) clearance where she was allowed to enter the military's "Sensitive Compartmented Information Facility" only to see the classified documents for action. However, she was able to illegally download a huge trove of documents on 5 January 2010, which she then transferred into her own personal computer. Later she went on downloading more documents and transferred them to Wikileaks Drop Box through TOR, a free overlay network enabling anonymous communication. President Barack Obama commuted her prison sentence and on March 13, 2020, she was released from prison. The Guardian reported on 22 October 2022 that her main motivation for leaking was because she felt that the military was misleading the American public about the Iraq War.

(c) **Edward Snowden** took advantage of the National Security Agency (NSA)'s system of allowing access to 1,000 "System Administrators", most of them contractors. As an intelligence official cited by *ABC News* said then: "It's 2013 and the NSA is stuck in 2003 technology." In that outdated system, Snowden, then working for an NSA contractor in Honolulu, had direct access to NSA's Fort Meade server.

(d) **Reality Leigh Winner**, who at 25 years old was working for an NSA intelligence contractor in Georgia, leaked official secrets out of a wrong sense of "patriotism". Earlier she had worked in the US Air Force for 6 years as a cryptologist linguist (Persian-Dari) and was assigned to the drone programme. After an honourable discharge from the Air Force, she was employed in 2016 by Pluribus Corporation, a private contractor working for the NSA, to translate Iran's aerospace documents. However, she went beyond her charter when she saw an NSA document on Russian interference in the 2016 US Presidential elections. It stated that the Russian Chief Intelligence Office had executed a cyber-attack on US voting software and sent "spear phishing" emails to more than 100 election officials just before the 2016 November elections. Out of "patriotic" considerations, she sent the document anonymously to *The Intercept*, which published it before the NSA verified its authenticity. The FBI was informed, she was arrested, tried, and sentenced.

Glenn Gerstell, who was General Counsel (2015-2020) for the NSA, has been quoted by *USA TODAY* as saying that the whole system of security clearances has gone out of control: "But maybe all these millions of people don't need access to everything the way we've got things going now".

5. OUTDATED SECURE COMMUNICATIONS

Government bureaucracies, including security services, are inelastic in their operations and often not able to keep pace with technological advances to update their security procedures. Consequently, they are not able to plug loopholes which allow "leakers" to communicate with non-authorised people. The system of using only official e-mails controlled/monitored by special servers has failed to plug loopholes. Many still use unauthorised e-mails.

The first person to flag this issue was Seymour Hersh in 1999, well before 9/11, who lamented that the US NSA, which was a technology catalyst during the Cold War, had become a technology resistant organisation. In his piece "The Intelligence Gap" (*New Yorker*, December 6, 1999), he noted: "The National Security Agency, whose Cold War research into code breaking and electronic eavesdropping spurred the American computer revolution, has become a victim of the high-tech world it helped to create" (Hersh, 1999).

On the other hand, the *Tech Evaluate* website reminds us that the first prototype of our cell phone was designed in the 1970s for the US military by Dr Martin Cooper of Motorola. He made the first call on 3 April 1973. It might surprise the present generation to know that the cell phone designed by him only allowed incoming calls and took 10 hours to charge for 30 minutes of talk time! In 2024 the cell phones we use are minicomputers which can perform several tasks besides phone calls (Mortensen, n.d.).

The dangers of using Artificial Intelligence (AI) in communications have been widely publicised, calling for global control through international laws. In brief, the dangers of misuse of AI are deep fakes, impersonation, reputational damage, more sophisticated cyber-attacks, data manipulation, automatic malware, and physical safety (Malwarebytes, n.d.).

The situation was recently described by Arvind Saxena, former Chairman of the Union Public Service Commission (India): "Today by placing everything online and permitting private players to collect and process data, we have provided free access to all critical information for unauthorised use. The people have been rendered transparent and vulnerable while big corporates have created walls of secrecy around themselves. The more data we collect and process on activities of our citizens the more vulnerable the nation becomes to its misuse by big players, foreign agencies and global as well as domestic corporates" (Saxena, 2024).

6. POLITICISATION OF STATE SECRETS

In some governments, there is a tendency by some "open" wings to assume responsibility over secret state to state negotiations without following necessary security precautions, or to misuse secret papers for political ends.

Nothing illustrates this better than an incident involving secret Libyan negotiations with Israel to improve relations. On August 28, 2023, Libyan Foreign Minister Najla el-Mangoush had to flee to Turkey for her safety when violent demonstrations started in Tripoli and other cities after an announcement by the Israeli Foreign Ministry that she had met Israeli Foreign Minister Eli Cohen in Rome. Israel had clearly violated what former Mossad chief (1989-1996) Shabtai Shavit said in his memoir: "Delicate diplomacy must begin with clandestine contacts." As a result, Prime Minister Benjamin Netanyahu had to publicly rebuke Cohen on August 30 and order that all sensitive public statements be cleared by him (Wintour, 2023).

Another politician who came to grief for mishandling secret intelligence papers is former Pakistan Prime Minister Imran Khan, who had frosty relations with the US and with the Pakistan Army. On 8 March 2022, the Pakistan opposition parties moved a motion of no-confidence in Khan's government in Parliament. By that time rumours were circulating that the US government was keen to oust Khan from his office because of his alleged proximity with Russia after the Ukraine War.

To counter this, Khan displayed a document at a public rally on 27 March and indicated it was evidence of a foreign conspiracy against his government. On 10 April he sent, against the advice of his law ministry, the original classified diplomatic cable on a meeting between the Pakistan Ambassador to the United States and two State Department officials on 7 March 2022, to the Chief Justice of Pakistan and alleged that it was evidence that the US had used Pakistan's envoy to send a threatening message to

him. His subsequent attempt to dissolve parliament was overruled by the Pakistan Supreme Court and Khan became the first Pakistan prime minister to lose office through a parliament vote (BBC, 2022).

On August 9, 2023, *The Intercept* published a report "Secret Pakistan Cable documents US pressure to remove Imran Khan" (Grim & Hussain, 2023). It said that a meeting between Pakistani ambassador to the United States and two State Department officials on March 7, 2022, had been the subject of "intense scrutiny, controversy, and speculation in Pakistan over the past year and a half." Following Khan's ouster, the Pakistan Federal Investigating Agency filed a case against him under the Official Secrets Act for mishandling a classified cable. Already serving a jail term for an unrelated corruption conviction, Khan was sentenced to 10 years imprisonment on 30 January 2024 (Fraser & Davies, 2024). On 3 June 2024, a Pakistani high court overturned the conviction (Reuters, 2024).

CONCLUSION

A study of history reveals that government secrets are regularly exposed by interested parties despite precautions taken by the originating end. This is because spying and betrayal are two sides of the same coin as war and peace.

Kautilya's *Arthashastra*, an ancient Sansrkit treatise on statecraft written around the 3rd century BCE, emphasises the important roles spies play in securing and defending a country. Among the principles of intelligence he discusses are placing secret agents for early detection in one's own country, an enemy country, a friendly country, and a neutral country to discover the strengths and weaknesses of each country. *Arthasastra* thus suggests that a king should employ "Five Eyes" as "static watchers" (Samstha) and four types of "moving watchers" (Samchar) with appropriate "covers" to detect foreign spies and traitors.

Similarly Sun Tzu (475-221 BCE) has written: "There are five kinds of spies: the local spy, the inside spy, the reverse spy, the dead spy and the living spy…it is essential for a leader to know about the five kinds of espionage, and this knowledge depends on reverse spies, so reverse spies must be treated well." Given what we have since learnt about double agents, Sun Tzu might also have meant that "reverse spies" (double agents) hired from among enemy spies needed more careful watch.

And if they were writing for our modern era, both sages would also have recommended that much more care be taken to protect the digital dissemination and transmission of sensitive information.

ABOUT THE AUTHOR

Vappala Balachandran
served as a high level national intelligence analyst and policy adviser to the Government of India, retiring as Special Secretary in the Cabinet Secretariat. His latest book is *Intelligence Over Centuries* published in 2022.

All views expressed in this article are personal views of the author.

REFERENCES

Aktaş, Alperen. (2023, October 23). *China calls Five Eyes intelligence alliance a 'security threat'*. Anadolu Agency. Retrieved from https://www.aa.com.tr/en/asia-pacific/china-calls-five-eyes-intelligence-alliance-a-security-threat-/3030201

Ashraf, A., Muhammad, A., Fazal, Z., Zeeshan, N., & Shafiq, Y. (2023). The role of civil society organizations in fostering equitable vaccine delivery through COVAX. *Eastern Mediterranean Health Journal, 29*(4), 232-235.

Balachandran, Vappala. (2023, January 22). Demystifying the master spies. *National Herald*. Retrieved from www.nationalheraldindia.com/opinion/demystifying-the-master-spies.

Balachandran, Vappala. (2022). *Intelligence Over Centuries*. Mumbai: Indus Source Books.

Balachandran, Vappala. (2014). *National Security & Intelligence Management: a new Paradigm*. Mumbai: Indus Source Books.

Baquet, D., & Keller, B. (2006, July 1). When do we publish a secret. *The New York Times*. Retrieved from www.nytimes.com/2006/07/01/opinion/01keller.html.

BBC. (10 April 2022). *Imran Khan ousted as Pakistan's PM after vote*. Retrieved from www.bbc.com/news/world-asia-61055210.

Braw, Elisabeth. (2021, June 4). Spying on allies is normal. Also smart. *Politico*. Retrieved from https://www.politico.eu/article/spying-allies-normal-us-denmark/

Carnegie Civic Research Network. (2021, September 30). *Civil Society and the Global Pandemic: Building Back Different?* Retrieved from carnegieendowment.org/2021/09/30/civil-society-and-global-pandemic-building-back-different-pub-85446.

Center for Strategic and International Studies. (n.d.). *Survey of Chinese Espionage in the United States since 2000*. Retrieved from www.csis.org/programs/strategic-technologies-program/survey-chinese-espionage-united-states-2000.

Corera, Gordon. (2024, May 15). China's spy threat is growing, but the West has struggled to keep up. *BBC*. Retrieved from https://www.bbc.com/news/articles/cmm33rm32veo

Disclose. (2019, April 15). *Yemen Papers*. Retrieved from made-in-france.disclose.ngo/en/chapter/yemen-papers/.

FBI. (2020, February 10). *Chinese Military Hackers Charged in Equifax Breach: Intrusion Affected Nearly Half of All Americans*. Retrieved from https://www.fbi.gov/news/stories/chinese-hackers-charged-in-equifax-breach-021020

Foster, Jackson. (2020, July 10). *The Hidden World of Holy Spies: A Q&A with NEH Public Scholar Matthew Avery Sutton*. Retrieved from www.neh.gov/blog/hidden-world-holy-spies-qa-neh-public-scholar-matthew-avery-sutton.

Fraser, S. & Davies, C. (2024, January 30). Imran Khan: Pakistan former PM jailed for 10 years in state secrets case. *BBC*. Retrieved from www.bbc.com/news/world-asia-68138591.

Global Times. (2024, March 26). *The slander by the Five Eyes alliance is just a clumsy political farce*. Retrieved from https://www.globaltimes.cn/page/202403/1309567.shtml

Goodman, J. & Mustian, J. (2024, February 16). Red flags, missed clues: How accused US diplomat-turned-Cuban spy avoided scrutiny for decades. *Associated Press*. Retrieved from apnews.com/article/cuba-spying-ambassador-diplomat-communism-miami-fbi-cia-2b065bd90e7576d9fff8adc4fa9c981f.

Grim, R. & Hussain M. (2023, August 9). Secret Pakistan cable documents US pressure to remove Imran Khan. *The Intercept*. Retrieved from theintercept.com/2023/08/09/imran-khan-pakistan-cypher-ukraine-russia/

Hersh, Seymour M. (1999, November 28) The Intelligence Gap. *The New Yorker*. Retrieved from www.newyorker.com/magazine/1999/12/06/the-intelligence-gap.

International Consortium of Investigative Journalists. (2021, October 27). *Pandora Papers journalists face government backlash for investigating financial secrecy*. Retrieved from www.icij.org/investigations/pandora-papers/pandora-papers-journalists-face-government-backlash-for-investigating-financial-secrecy/.

Malwarebytes. (n.d.) *AI in Cyber Security: Risks of AI*. Retrieved from www.malwarebytes.com/cybersecurity/basics/risks-of-ai-in-cyber-security.

Sun Tzu. *Art of War XIII: On the Use of Spies*. Translated by the Massachusetts Institute of Technology. Retrieved from web.mit.edu/~dcltdw/AOW/13.html.

Mortensen, John (n.d.) *Why is technology evolving so fast*. Retrieved from techevaluate.com/why-is-technology-evolving-so-fast/.

Monat, Pawel, & Dille, John. (1962). *Spy In The U.S*. Retrieved from https://www.cia.gov/readingroom/docs/CIA-RDP80B01676R002600060013-6.pdf

NBC News. (2008, May 30). *Did Chinese hack Cabinet secretary's laptop*. Retrieved from www.nbcnews.com/id/wbna24880526.

Open Source Center. (2009, June 30). *Jihadist Website Posts Al-Libi's "Guidance on the Ruling of the Muslim Spy"*. Retrieved from irp.fas.org/dni/osc/libi.pdf.

Pelley, Scott. (2023, October 22). China stealing technology secrets – from AI to computing and biology, "Five Eyes" intelligence leaders warn. *CBS News*. Retrieved from https://www.cbsnews.com/news/china-stealing-technology-secrets-five-eyes-intelligence-leaders-warn-60-minutes-transcript/

Reuters. (2024, June 3). *Pakistan's Imran Khan acquitted of leaking state secrets charges, but to stay in jail*. Retrieved from https://www.reuters.com/world/asia-pacific/pakistan-court-suspends-former-pm-imran-khans-sentence-state-secrets-case-ary-2024-06-03/

Rustagi, N., & Wu, A. (2020, October 30). Indian Civil Society Sidelined in a Pandemic. *East Asia Forum*. Retrieved from eastasiaforum.org/2020/10/30/indian-civil-society-sidelined-in-a-pandemic/.

Saxena, Arvind. (2024, February 7). Perils of IT~II. *The Statesman*. Retrieved from www.thestatesman.com/opinion/perils-of-itii-1503267358.html#google_vignette.

Tait, Robert. (2023, December 10). 'Ego and resentment': what led former US diplomat to spy for Cuba? *The Guardian*. Retrieved from https://www.theguardian.com/world/2023/dec/10/ego-and-resentment-what-led-former-us-diplomat-to-spy-for-cuba

US Department of Justice. (2020, August 17). *Former CIA Officer Arrested and Charged with Espionage*. Retrieved from www.justice.gov/opa/pr/former-cia-officer-arrested-and-charged-espionage.

Welsh, Teresa. (2015, September 25). Obama, Xi reach agreement to end cyberattacks. *US News*. Retrieved from www.usnews.com/news/articles/2015/09/25/president-obama-chinese-president-xi-jingping-announce-agreement-to-stop-hacking.

Willsher, Kim. (2023, September 19). France accused of attack on press freedom after journalist arrest. *The Guardian*. Retrieved from www.theguardian.com/world/2023/sep/19/france-accused-attack-press-freedom-journalist-arrest.

Wintour, Patrick. (2023, August 30). Libyan foreign minister flees country amid outcry over meeting with Israeli counterpart. *The Guardian*. Retrieved from www.theguardian.com/world/2023/aug/30/libyan-foreign-minister-flees-country-amid-outcry-over-meeting-with-israeli-counterpart.

Wray, Christopher. (2020, July 7). *The Threat Posed by the Chinese Government and the Chinese Communist Party to the Economic and National Security of the United States*. Retrieved from https://www.fbi.gov/news/speeches/the-threat-posed-by-the-chinese-government-and-the-chinese-communist-party-to-the-economic-and-national-security-of-the-united-states

Yilek, Caitlin. (2024, February 14). Former US ambassador accused of spying for Cuba for decades pleads not guilty. *CBS News*. Retrieved from www.cbsnews.com/news/victor-manuel-rocha-diplomat-spy-cuba/.

NAVIGATING THE DEEPFAKE DILEMMA:
TRENDS, THREATS AND MITIGATION STRATEGIES

Asha Hemrajani
S. Rajaratnam School of International Studies (RSIS), Singapore

ABSTRACT

Deepfakes are a type of synthetic media – media content generated or changed in some way by Artificial Intelligence (AI) – that resemble certain persons, items, locations or events and may falsely appear to a viewer to be genuine. As deepfakes become more widespread, it will be more and more difficult to distinguish between information created by humans and content produced by AI, which would facilitate unlawful and dangerous activities. The dilemma that arises when debating how to address deepfakes is how to effectively manage the nefarious uses of synthetic media while not discouraging or hindering the significant economic opportunities and positive uses such AI-generated media also creates. The key is in deploying a range of mitigation techniques, described in this article, that can help suppress the impact of negative use. It is important to note that these methods are not foolproof. Our focus also needs to be on how to build our social resilience as a way to address the dangers arising from deepfakes.

WHAT ARE DEEPFAKES?

In December 2023, during a Q&A session with the Russian public, Russian President Vladimir Putin was visibly surprised when he was asked a question by someone who appeared to look exactly like him. It turned out to be a student from St Petersburg who was using an AI-generated deepfake video of Putin to ask him a question live (Suciu, 2023), presumably to make his point about the prevalence of deepfakes and for shock value.

What are deepfakes and why did this particular one cause such a stir?

Nina Schick, a renowned global Generative AI expert, describes deepfakes in her book *Deepfakes: The Coming Infocalypse* as "a type of 'synthetic media' meaning media (including images, audio and video) that is either manipulated or wholly generated by AI" (Schick, 2020). The European Union (EU)'s Artificial Intelligence Act, which sets comprehensive rules for the responsible and safe use of AI in the EU, defines deepfakes as "AI generated or manipulated image, audio or video content that resembles existing persons, objects, places or other entities or events and would falsely appear to a person to be authentic or truthful."[1]

The most commonly known deepfake technique is swapping one person's face with another's. Deepfakes are becoming more widespread thanks to the following factors: easily accessible AI, readily available web applications and mobile apps, abundance of freelancers and experts who can generate deepfakes as a service, and advancing wireless connectivity such as 5G networks (Hemrajani, 2023).

This "synthetic media" and its incorporation with other AI capabilities can have the potential to both create significant economic opportunities while also

[1] The EU's AI Act, which was unanimously endorsed by all 28 member states in February 2024 and passed by the EU Parliament on 13 March 2024, came into force on 1st August 2024. For text of the legislation, see https://artificialintelligenceact.eu/wp-content/uploads/2024/01/AI-Act-Overview_24-01-2024.pdf

posing serious threats to society. This is because it is becoming more difficult to distinguish between information created by humans and content produced by AI, which might facilitate unlawful and dangerous activities. What if the deepfake impersonation of Putin had been used for more sinister purposes instead of just a joke meant to shock?

This article thus seeks to examine both the positive and negative uses of synthetic media, both current and potentially in the future as AI continues to develop. Due to the fears surrounding the abuse of synthetic media, there is an increasing inclination towards introducing guidelines and even legislation to regulate synthetic media. This article further seeks to examine the effectiveness of deepfake legislation and other ways to mitigate the risks arising out of deepfakes.

POSITIVE USES OF SYNTHETIC MEDIA

There are multiple sectors such as training, education, art, and medical science where synthetic media can be put to good use by performing automatic language translation, marketing, entertainment and customer services functions.

One potential positive use of synthetic data is the generation of medical imaging datasets for the AI-based diagnosis of critical diseases such as tumorous cancers. AI deep learning tools require a significant amount of wide-ranging data to make the AI-based tool effective. As pathologic (positive for cancer) results are not that common in medical imaging datasets, scientists have suggested generating fake abnormal scans of brain tumours to better train AI tools to spot tumours more effectively. This will address two challenges with using data to train models, namely: a) increasing the number of abnormal images for better training of models, and b) protecting the privacy of cancer-stricken patients so that their real images do not need to be used for AI models (Shin, 2018).

AI companies such as *vocalid.ai* create audio recordings of AI generated voices for multiple purposes such as radio and TV ads, in-store announcements and ads, podcast promos etc. AI generated voices also give people who have lost their voices due to illness an opportunity to "speak". Another AI company *synthesia.io* generates high quality videos with their database of AI avatars that can speak in over 100 languages. It was used by the UK non-profit organisation that, with the footballer David Beckham, created a video to raise awareness about malaria (Davies 2019). In the 54-second video, Beckham is speaking in nine different languages and his lips are well in sync with the language being spoken.

Another startling positive use case is in the Dali Museum in Florida in the United States which made a "life-size re-creation" of Salvador Dali in 45 minutes of new video with multiple combination possibilities to help visitors to the museum obtain a more enriching experience (Lee, 2019).

Computer-Generated Imagery, or CGI, has long been the main technology behind special visual effects in movies and TV shows. Deepfakes are now emerging as the innovative and cheaper challenger to CGI and are beginning to play a role in the film and TV industry (EISKO, n.d).

NEGATIVE USES OF SYNTHETIC MEDIA – DEEP FAKES

Deepfakes are also increasingly and alarmingly being used for nefarious purposes. There are four categories where deepfakes can be used harmfully: 1) impersonation (for disinformation and commercial crime), 2) military deception, 3) harassment/revenge porn, and 4) Liar's Dividend (Hemrajani, 2024).

1. Impersonation

Impersonation for the purposes of political and information campaigns

Freedman (2023) defines information campaigns as "an attempt by an individual or a group – which could be a state – to establish, shape or challenge a narrative; this effort may encompass what could be described as… 'disinformation'". Deepfakes are increasingly being used to propagate information campaigns or disinformation, both in times of war and elections.

A notable deepfake impersonation video is that of Ukrainian President Volodymyr Zelenskyy asking his soldiers to surrender, supposedly created by Russia as part of its disinformation campaign against Ukraine (Allyn, 2022).

In December 2023, the *Financial Times* reported that in the run-up to the general elections in Bangladesh, a deepfake video, which showed an opposition leader Tarique Rahman hesitating about supporting the people of Gaza, was posted on Facebook. In light of the current Israel Hamas conflict, this would not have boded well for the opposition party in a country like Bangladesh where the public is likely to have strong sympathy for the Palestinians (Parkin, 2023).

There have been many other such examples of deepfakes being used in elections to either portray one party in a positive light or the opposition party/ candidate in a negative light.

There also have been many instances of politicians using deepfakes to generate synthetic images to help with their campaign advertisements and fundraising activities, ranging from innocuous ones for self-promotion to those that paint doomsday scenarios should their opposition be elected such as when the US Republican Party released a deepfake video of what would happen if President Biden were re-elected. The video consisted of "AI-generated images portraying what an apocalyptic Biden-Harris second term would look like. The video – a part of the RNC's Beat Biden campaign – featured images of rundown, collapsed Wall Street buildings, war and explosions in Taiwan and police in tactical gear defending San Francisco from crime" (Johnson, 2023).

As the CEO of IBM Arvind Krishna was reported saying in a *Wall Street Journal* in July 2023, "the problem of disinformation is hardly new, but AI compounds it. AI stands to increase the rate and pace and perhaps the power of disinformation campaigns. … More than that, I think the real worry is you can fine-tune them for every single audience" (Rosenbush, 2023).

Impersonation for the purposes of perpetrating commercial crime

There have been several examples where deepfake media has been leveraged to conduct commercial crime activities such as theft, money laundering and enticements to invest in investments schemes via impersonation.

In May 2023, just five months after China launched new regulations to govern deepfakes (see legislation section below), *Reuters* reported a case of a man in Inner Mongolia duped into transferring a large sum of money to a criminal who had impersonated the victim's friend via the use of AI-generated deepfake on a video call (Reuters, 2023).

Financial institutions have long been required to conduct Know Your Customer (KYC) verification. This is mainly to comply with regulations on money laundering and terrorism financing. Online KYC verifications also help with preventing scams and fraud. It is therefore an important and required step when opening an online bank account, for example. The account user must be present during a live video call so that his "liveness" can be confirmed. Criminals can, however, use deepfake videos to pass these online KYC checks, which let them create accounts for illegal activities without letting the true identity of the account holder be known. An AI fraud detection solution provider, *sensity.ai*, has reviewed the commonly used online KYC verification solution providers and found that "the vast majority were severely vulnerable to deepfake attacks." This means that criminals can use deepfakes to get around the security checks that are built into KYC systems and continue to move funds around for their illegal activities.

In Singapore, deepfake impersonation videos of then Deputy Prime Minister Lawrence Wong and then Prime Minister Lee Hsien Loong began appearing in late 2023. In the deepfake video of Mr Lee that was created from footage of an interview with him on the Chinese news network CGTN, he speaks of "an investment opportunity purportedly approved by the Singapore government" (Ng, 2023). The video represents a misuse of the then Prime Minister's image to promote what are likely shady investment opportunities.

Deepfakes are also being used for extortion and blackmail, as reported by several Members of the Singapore Parliament. In April 2024, Member of Parliament Edward Chia wrote on his Facebook page that he had received a letter containing a "distasteful photo where my face was digitally manipulated onto one of the figures, accompanied by an extortion demand". Adding that he had made a police report, he noted that "the rise of deepfakes makes it harder to discern reality from fiction…[and] can pose a significant threat to our social fabric" (Ong, 2024).

2. Military deception

Deepfakes may be used for malicious purposes in military contexts, potentially undermining decision-making and hindering situational awareness, particularly during critical situations (Hemrajani 2024).

Meucci et. al. (2023) calls this "a new form of attack that digitally modifies the number and quality of military targets". Their study investigated the possibility of injecting malicious fake radar images into maritime navigational systems. Such manipulation can undermine navigational integrity in various ways. These fake images could generate fake targets, so the navy ship would be shooting at something that is not there. Or the images could conceal actual targets or other ships, like the Titanic not seeing the iceberg it hit. It could also lead to the military vessel changing its course (Meucci et. Al., 2023).

3. Harassment/Non-consensual manipulative pornography

Recent press reports (Krietzberg, 2024) have noted that a growing number of women have fallen victim to perpetrators creating deepfake pornographic images or videos of them and posting them online on social media. The technique used to create these synthetic media involves using already available pornographic materials and integrating the victim's face using AI to replace the original face.

The case creating the biggest uproar so far was the emergence in January 2024 of deepfake pornographic images of the well-known singer Taylor Swift that were posted on multiple social media forums (Sink, 2024).

The Taylor Swift images were created using Microsoft Designer, a design tool that can, amongst other capabilities, generate images based on users' prompts. Microsoft has since announced that they have "strengthened safety systems and closed the loopholes that enabled users to generate the images in the first place" (Krietzberg, 2024).

Another widely used and known tool used for this nefarious purpose is the DeepNude AI tool which is self-described as a tool to "undress photos of women and produce a realistic nude image." A version of this tool has been used from within the social messaging platform Telegram to generate a large quantity of explicit images of females which were subsequently widely distributed (Burgess, 2020).

Although the DeepNude AI tool has been blocked in multiple countries and Apple has already banned the Telegram bot on iPhones, a quick online search by the author uncovered many other such tools that have become available for use on Telegram.

4. Liar's Dividend

A far more nefarious scenario with the advent of deepfakes could be immediate distrust when consuming information. This may result in "Liar's Dividend" (Chesney and Citron, 2019) where "deep fakes make it easier for liars to avoid accountability for things that are in fact true". Increasing public awareness of deepfakes might cause some people or communities to doubt the veracity of a genuine video, which would make it simpler for those responsible to evade punishment. In fact, Chesney and Citron (2019) argue that as "deep fakes become widespread, the public may have difficulty believing what their eyes or ears are telling them – even when the information is real. In turn, the spread of deep fakes threatens to erode the trust necessary for democracy to function effectively."

A few of the accused standing trial for rioting on Capitol Hill in the US in January 2021 during the last days of President Trump's tenure attempted, but were unsuccessful, to use this advantage in court by claiming that the video footage was AI-produced (Bond, 2023).

A similar ruse was adopted by an Indian opposition party leader when damning audio clips of his voice were released by a politician from the ruling party. He denied the audio clips were of his voice and claimed they had been created by AI. Independent experts were brought in to analyse the clips, and they concluded that at least one of the clips was indeed authentic (Christopher, 2023).

WORSENING RISKS OF DEEPFAKES

With the discovery of more examples of deepfakes, debate and anxiety around deepfakes is increasing at a frenetic pace. The risks arising from deepfakes are twofold:

a) Human detection of deepfakes, whether video or audio, are not foolproof. Research findings suggest that people cannot always accurately identify deepfakes and tend to overestimate their own ability to detect them (Kobis et. Al., 2021).

b) As AI technology advances, the quality of deepfakes will improve. Hence, nefarious uses of deepfakes will not be restricted to the categories listed above and are likely to expand to other areas.

MITIGATION STRATEGIES

In the light of the worsening risks arising from deepfakes, what can be done to mitigate these risks? The dilemma that arises when debating how to address deepfakes is how to effectively manage the nefarious uses of synthetic media while not discouraging or hindering its positive uses. Another dilemma revolves around whether any action taken to tackle the nefarious uses of deepfakes would be effective at all or would simply be a losing battle given the lightning speed of AI development.

This paper discusses five different mechanisms to tackle deepfakes and their relative pros and cons. These include 1) awareness building/education, 2) legislation/regulatory frameworks, 3) tools, 4) multi-stakeholder fact-checking taskforces, and 5) strengthening our society and democracy. Each of these are examined in terms of potential effectiveness and future proof-ness at least in the mid-term.

1. Awareness Building/Education in Critical Thinking

There have been repeated calls for more education and awareness building where deepfakes are concerned, in the press, education and policy think-tank sectors. The question is how should this education and awareness building take place and which segments of society should it target?

First and foremost, swift reactions/responses when there has been an unauthorised use of images or videos to generate synthetic media and released publicly is an effective way to both raise awareness as well as to stem the influence and spread of the synthetic media. When then Prime Minister Lee Hsien Loong's deepfake images and videos of him promoting investment products emerged in 2023, he released a Facebook post in December 2023 urging Singaporeans to be "vigilant and learn to protect themselves and loved ones against deepfake scams" (Chiu, 2023).

Secondly, differentiated public education programmes targeting multiple segments of society who differ in age, language and IT savviness would be needed. Training could focus on helping end users of content sharpen their detection skills by incorporating online quizzes such as *Detect Fakes*, the online experiment designed by Northwestern's Kellogg School of Management for research purposes, in which users can test their knowledge on deepfake spotting (Kellogg, n.d.). Deepfakes training could be made mandatory for members of the press given their exposure and consumption of international media content.

The training could, for example, comprise the following components: a) an introduction to Generative AI and how it can be used to generate synthetic media both for positive and negative purposes, b) how synthetic media is distributed and spread, especially via social media, c) understanding the threats of misinformation that can arise from the spread of synthetic media, and d) distinguishing between genuine and synthetic media and the various tools and mechanisms to aid in this.

In many ways, critical thinking skills can serve as our best defense against the influence of deepfakes. By teaching people, especially the young, how to analyse information critically, susceptibility to deepfakes can be reduced. Such a curriculum should prioritise developing skills in evaluating evidence, identifying logical fallacies, and understanding media literacy. Moreover, it should emphasise the importance of corroboration, seeking multiple sources, and considering the context of information.

In Singapore, teaching critical thinking in schools has always been given great importance. In 1997, the "Thinking School, Learning Nation" concept was introduced. This was followed by the Ministry of Education's "Teach Less, Learn More" (TLLM) initiative in 2005 whose goal was, among other things, to nurture critical thinking (Loo, 2018).

Going forward, critical thinking skills can be given greater weightage in primary and secondary school curricula. It could, for example, be incorporated

across various subjects, not just as a standalone course. Additionally, assigning greater weightage to critical thinking skills in assessments can incentivise students to develop and apply these abilities effectively.

It is also gratifying to note that the Singapore National Library Board's S.U.R.E. (Source, Understand, Research, Evaluate) programme will continue its work on education to promote information discernment and this year will roll out its largest programme yet, which will focus on Generative AI and deepfakes in particular (National Library Board, n.d.).

However, with increased awareness building comes the risk of increased Liar's Dividend. As Chesney and Citron (2019) described in their paper in the California Law Review, "this dividend flows, perversely, in proportion to success in educating the public about the dangers of deep fakes". Hence as education initiatives on deepfakes increase, people could become more cynical and dismiss genuine news or content as deepfakes. However, it is this author's view that the benefits from training outweigh the risks of Liar's Dividend.

2. Legislation/Regulatory frameworks

In 2023, China was one of the first, if not the first country in the world to set out regulations specifically governing deepfakes. Called Deep Synthesis Provisions, these regulations govern two types of players in this market: the content generation service providers and the end-users The regulations stipulate that any synthetic content must be labelled with a watermark. The content generation service providers need to commit that they will not handle personal information, must get the real identities of their end-users, and set up feedback mechanisms for content consumers (Hemrajani, 2023).

Similarly, clause 70b of the EU AI Act stipulates that any deepfakes should "also clearly and distinguishably disclose that the content has been artificially created or manipulated by labelling the artificial intelligence output accordingly and disclosing its artificial origin."

Unlike the Chinese regulations, however, the EU AI Act does not mandate that deepfake content providers seek to verify the identity of their end users, the consumers of the deepfake content.

There are several limitations to these mitigation techniques for a country like Singapore. Firstly, unlike China, Singapore's data borders are porous. Hence the inflow of these deepfakes cannot be completely controlled. Secondly, enforceability against malicious content creators, especially those operating from outside of Singapore, would likely be an issue. Thirdly, current watermarking techniques have severe technical limitations. The integrity of watermarks can be compromised by manipulation, removal or alteration, casting doubt on whether the content is genuine or not (Leibowicz, 2023).

Singapore, like most other countries, does not currently have any legislation specifically targeting deepfakes. Some may argue that no new legislation to tackle deepfakes is needed in Singapore. This is because Singapore has enacted the Protection from Online Falsehoods and Manipulation Act (POFMA), whose main aim is to address false statements communicated in Singapore via the Internet. In her article on China's Deepfakes regulations, Hemrajani (2023) argues that while Singapore may already have POFMA, this piece of legislation "cannot, however, counter the production of manipulated content. These laws only kick in when the deepfake is distributed on the Internet." What if the synthetic media services operate offline? The key differentiator in the Chinese approach is that Chinese legislation imposes pre-emptive measures to address the issue at the source of the deepfake rather than wait for an offence to occur.

Another possible solution could be interim bans on deepfakes only during sensitive periods such as elections. The Korean national assembly, for instance, revised their elections laws to ban the usage of deepfakes in political campaigns close to the time of elections (Straits Times, 2024).

3. Tools

Software based tools are a critical component of the arsenal to help combat negative use cases. There are three possible types of tools in this arsenal: tools to ease the process of reporting observed deepfakes to a central authority, tools that help to verify the authenticity of the digital content, and tools that help to detect deepfakes.

a. Reporting

Reporting deepfakes is an important first step in the battle against malicious use cases. In the case of the deepfakes of then Prime Minister Lee, he urged the public to refrain from responding to such videos and instead report them to the integrated reporting channel such as ScamShield Bot illustrated below in Figure 1.

Reporting tools for the public must be designed with ease-of-use in mind, as the ScamShield Bot has been designed to be. Reporting and collating reports of potential abuses of synthetic media will go some way to help authorities understand better the types and frequencies of deepfakes that are circulating.

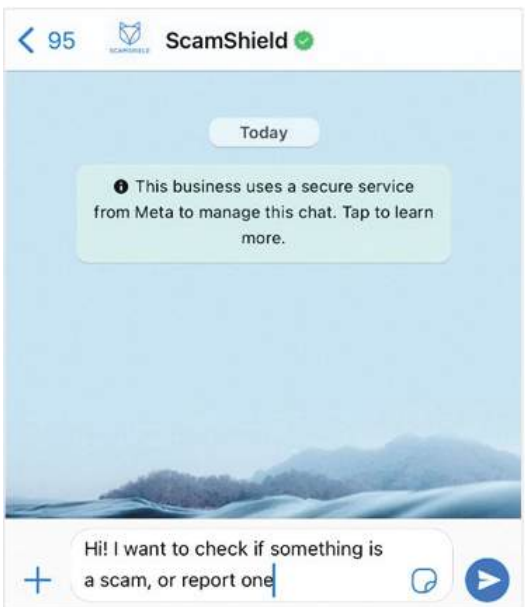


Figure 1. ScamShield Bot on WhatsApp

b. Digital Content Authenticity

In response to the growing number of incidences of manipulated image and video content, industry players have banded together to develop technical standards for the tracking of the origin and authenticity of digital media. The Coalition for Content Provenance and Authenticity (https://c2pa.org/), for example, has set up open standards to provide producers the means to indicate provenance (history and origin) data on content they have created. The standards can provide consumers of content the means (via the use of tools) to check the details of an image or a video so that they have the knowledge that the content has not been tampered with and is from whom it says it is from. These tools comprise open-source software libraries that allow content creators to verify or display credentials pertaining to their digital content (Content Authenticity Initiative, n.d.).

For digital content authenticity to be effective, news agencies, offline and online media as well as social media platforms should mandate the use of these open standards for all media used or posted. It would go a long way towards dampening the impact of the negative uses of synthetic media because consumers of such media will know that the content they are consuming has been verified.

c. Detection

There are currently a number of tools available commercially, of various levels of sophistication and accuracy, that help with deepfake detection. These tools allow users to upload digital media which is then analysed for manipulation. The tool, if effective, then indicates if and how the media has been manipulated. Some tools analyse images and videos of human beings for signs of blood flow on the face and other subtle changes undetectable by the human eye to determine their authenticity. Other tools compare the input media against a database of known deepfakes. And yet others look for mismatches between the spoken words on the video and actual lip movement.

However, detection tools face a serious challenge: they are not foolproof and no one tool can detect all types of deepfakes as there are a variety of ways to create fakes and a variety of ways to detect them. Intel, one of the world's leading technology conglomerates, launched their tool *FakeCatcher* which was put to the test by the BBC with mixed results. It was able to detect the genuinely fake videos but falsely labelled authentic videos as fake (Clayton, 2023). This can lead to the Liar's Dividend problem.

Initiatives devoting more resources to developing better tools are underway that can hopefully address this challenge. On 10 January 2024, Singapore's Minister for Communications and Information Josephine Teo announced a new initiative to

foster online trust and safety by developing tools to tackle deepfakes. The detection, watermarking and content authentication tools will be developed by the Centre for Advanced Technologies in Online Safety (CATOS) (Lee, 2024). CATOS, which will receive $50million in funding, is "developing plug-ins and software solutions that can seamlessly include content provenance when publishing articles or images" (Abdullah, 2024).

But would awareness building, legislation and tools suffice?

The fact is deepfakes are growing in sophistication, and it will be a perpetual cat and mouse/catchup game where tools and legislation are concerned. There may possibly be a perennial chain of loopholes or misinterpretations where legislation is concerned. New types of deepfakes may pop up that fail to be detected by detection tools. Or sophisticated cutting-edge tools may not be made available to the people or organisations who need them most due to cost, intellectual property and/or other concerns. Hence, two additional mechanisms described below could be considered in conjunction with the above three.

4. Multi-stakeholder fact-checking taskforces

Getting access to the latest tools to combat deepfakes is not guaranteed and even if access is obtained, training is required to know how to use the tools effectively.

Witness, a US-based NGO, has set up the *Deepfakes Rapid Response Force*, a multi-stakeholder taskforce, to address the accessibility and capacity building challenge related to tools (Witness, n.d.). The taskforce will work on fact-checking by leveraging and bringing together journalists, fact-checkers, researchers in media forensics, experts in deepfakes, news gathering as well as open-source intelligence (OSINT) verification to review content (UK Parliament, 2023).

This multistakeholder taskforce model can be customised and adopted for various sectors and regions.

An entity along similar lines has been set up in Singapore where a volunteer-run, self-funded crowd-sourced service called CheckMate can fact-check content that users of the service send in (Abdullah, 2024).

5. Strengthening our society by building social resilience

There is a school of thought that deepfakes and the disinformation generated do not create rifts in society, they merely exploit the pre-existing rifts in society. Silbey (2019) argues in her paper "The Upside of Deep Fakes" that "deep fakes don't create new problems so much as make existing problems worse. Cracks in systems, frameworks, strategies, and institutions that have been leaking for years now threaten to spring open. Journalism, education, individual rights, democratic systems, and voting protocols have long been vulnerable. Deep fakes might just be the straw that breaks them."

In an effort to protect the integrity of information, governments are actively working to create new legislation and regulations, along with requiring watermarking of deepfakes in order to help the public identify them. However, while rules and technology are crucial, they have limitations (Rosenbush, 2023).

Hence, because of these limitations, Silbey (2019) suggests the "effective way to respond to the scourge of deep fakes isn't to target the creation and use of deep fakes themselves, but rather to focus on strengthening the social and political institutions they disrupt. Now would be a good time to focus on *institutional inoculation, fortitude, redundancy, and resiliency* [emphasis added]". If as a society, we develop and continue to foster our cohesion and resilience, we will be able to withstand even the most insidious of deepfakes.

CONCLUSION

With the advent of AI, synthetic media is here to stay. While there are many good use cases for synthetic media, the rising number of illegal, fraudulent, and harmful use cases of synthetic media misuse across various categories is cause for concern. The dilemmas that arise when debating how to address deepfakes is how to effectively manage the nefarious uses of synthetic media while not discouraging or hindering its positive uses, and if mitigation techniques actually work. The key is in deploying a range of mitigation techniques in combination that

can help suppress the impact of negative use. This includes education, awareness building, deploying tools to help with reporting incidents of deepfakes, digital content authentication and detection of sophisticated deepfakes. These methods are, however, not entirely foolproof. The deployment of multi-stakeholder fact-checking taskforces is a viable option. Ultimately, however, our focus also needs to be on how to build our social resilience to address the dangers of deepfakes.

ABOUT THE AUTHOR

Asha Hemrajani
is Senior Fellow at the Centre of Excellence in National Security (CENS) at the S Rajaratnam School of International Studies (RSIS) at Nanyang Technological University (NTU). Her research interests include Artificial Intelligence (AI) safety and governance, information and data security, digital economies and supply chain challenges, critical information infrastructure (CII), cybersecurity and corporate governance. Ms. Hemrajani has over 20 years of tech and business experience, spanning network engineering, strategy, regulatory in the mobile communications, domain names and cybersecurity sectors. She was formerly a member of the Board of Directors at ICANN, the global domain names regulator. She has a bachelor's degree in electrical engineering and a ModularMaster in cybersecurity by design.

REFERENCES

Abdullah, Zhaki. (2024, May 16). Got a text that you think is a scam? S'pore's new centre to fight online harms can help verify it. *The Straits Times*. Retrieved from https://www.straitstimes.com/tech/centre-to-help-singapore-fight-online-harms-launched-gets-50m-funding

Allyn, Bobby. (2022, March 16). Deepfake video of Zelenskyy could be 'tip of the iceberg' in info war, experts warn. *npr*. Retrieved from npr.org.

Bond, Shannon. (2023, May 8). People are trying to claim real videos are deepfakes. The courts are not amused. *npr*. Retrieved from npr.org.

Burgess, Matt. (2020, November 17). The AI Telegram bot that abused women is still out of control. *WIRED*. Retrieved from wired.co.uk.

Chesney, Bobby and Citron, Danielle. (2019). Deep Fakes: A Looming Challenge for Privacy, Democracy, and National Security. California Law Review, Volume 107, retrieved from californialawreview.org.

Chiu, Christie. (2024, January 4). PM Lee warns against responding to deepfake videos of him promoting investment scams. *The Straits Times*. Retrieved from straitstimes.com.

Christopher, Nilesh. (2023, July 5). An Indian politician says scandalous audio clips are AI deepfakes. We had them tested. *Rest of world*. Retrieved from restofworld.org.

Clayton, James. (2023, July 23). Intel's deepfake detector tested on real and fake videos. *BBC News*. Retrieved from bbc.com.

Content Authenticity Initiative. (n.d.) *CAI open-source SDK*. Retrieved from https://opensource.contentauthenticity.org/

Davies, Guy. (2019, April 10). David Beckham 'speaks' 9 languages for new campaign to end malaria. *abcNEWS*. Retrieved from abcnews.go.com.

Kellogg School of Management, Northwestern University. (n.d.) AI-generated or Real? *Detect Fakes*. Retrieved from https://detectfakes.kellogg.northwestern.edu

EISKO. (n.d.). *Deepfake vs. traditional CGI*. Retrieved from https://eisko.com/2023/11/27/deepfake-vs-traditional-cgi/#:~:text=Deepfakes%2C%20a%20portmanteau%20of%20%E2%80%9Cdeep,audio%20content%20with%20stunning%20accuracy

European Commission. (2024, January). AI Act: Full text. Artificial Intelligence Act. Retrieved from https://artificialintelligenceact.eu/wp-content/uploads/2024/01/AI-Act-FullText.pdf

European Union. (2024, 11 March). *Briefing on the Artificial Intelligence Act*. Retrieved from https://artificialintelligenceact.eu/wp-content/uploads/2024/01/AI-Act-Overview_24-01-2024.pdf

Freedman, Lawrence and Williams, Heather. (2023). *Changing the Narrative Information Campaigns, Strategy and Crisis Escalation in the Digital Age*. UK. Routledge.

Hemrajani, Asha. (2024). *Cyber and Information Threats in the Age of AI* [Unpublished internal report]. S Rajaratnam School of International Studies.

Hemrajani, Asha. (2023). China's New Legislation on Deepfakes: Should the Rest of Asia Follow Suit? *The Diplomat*. Retrieved from thediplomat.com.

Johnson, Arianna. (2023, April 25). Republicans Share an Apocalyptic AI-Powered Attack Ad Against Biden: Here's How to Spot a Deepfake. Forbes. Retrieved from forbes.com.

Kobis, Nils. (2021). Fooled twice: People cannot detect deepfakes but think they can. *iScience*. Volume 24, 103364, pages 1-2.

Krietzberg, Ian. (2024, February 3). Deepfake porn: It's not just about Taylor Swift. *The Street*. Retrieved from thestreet.com.

Lee, Dami. (2019, May 10). Deepfake Salvador Dalí takes selfies with museum visitors. *The Verge*. Retrieved from theverge.com.

Lee, Li Ying. (2024, January 11). New $20m initiative in S'pore to develop tools to detect deepfakes and misinformation. *The Stratis Times*. Retrieved from straitstimes.com.

Leibowicz, Claire. (2023, August 9). Why watermarking AI-generated content won't guarantee trust online. *MIT Technology Review*. Retrieved from technologyreview.com.

Loo, Janice. (2018, March 19). *Teach Less, Learn More*. Singapore Infopedia. Retrieved from https://www.nlb.gov.sg/main/article-detail?cmsuuid=bf38bb79-2b26-4068-828c-c89246c65c10

Meucci, Guilio et al. (2023). Naval Cybersecurity in the Age of AI: deceptive ISAR Images Generation with GANs. *IEEE* (early-stage research, not yet published). researchgate.net/publication/374807357_Naval_Cybersecurity_in_the_Age_of_AI_deceptive_ISAR_Images_Generation_with_GANs.

National Library Board. (n.d.). *Be S.U.R.E. Together About Gen AI and Deepfakes at NLB's Largest Information Literacy Outreach To Date*. Retrieved from https://www.nlb.gov.sg/main/about-us/press-room-and-publications/media-releases/2024/Be-SURE-Together-about-Gen-AI-and-Deepfakes

Ng, Hong Siang and Hamzah, Firdaus. (2023, December 29). Deepfake video of PM Lee emerges amid growing prevalence of manipulated content. *today*. Retrieved from todayonline.com.

Ong, Su Mann. (2024, April 21). MP receives 'distasteful photo where my face was digitally manipulated onto one of the figures'. *STOMP*. Retrieved from https://stomp.straitstimes.com/singapore-seen/mp-receives-distasteful-photo-where-my-face-was-digitally-manipulated-onto-one-of-the

Parkin, Benjamin. (2023, December 14). Deepfakes for $24 a month: how AI is disrupting Bangladesh's election. *Financial Times*. Retrieved from ft.com.

Rosenbush, Steven. (2023, July 28). Pro Take: Tech Executives Call for Critical Thinking to Counter Deepfakes, Disinformation. *The Wall Street Journal*. Retrieved from wsj.com.

Schick, Nina. (2020). *Deepfakes The Coming Infocalypse*. New York: Hachette Book Group

Shin, HC. et al. (2018). Medical Image Synthesis for Data Augmentation and Anonymization Using Generative Adversarial Networks. In: Gooya, A., Goksel, O., Oguz, I., Burgos, N. (eds) *Simulation and Synthesis in Medical Imaging. SASHIMI 2018. Lecture Notes in Computer Science*, vol 11037. Springer.

Silbey, Jessica. (2019). The Upside of Deep Fakes. *Maryland Law Review*, Volume 78 (Issue 4).

Sink, Justin. (2024, January 29). White House deplores 'alarming' sexually-explicit AI-generated images of Taylor Swift, urges social media companies to enforce 'their own rules'. Fortune. Retrieved from fortune.com.

Staff Writer. (2023, May 22). 'Deepfake' scam in China fans worries over AI-driven fraud. *Reuters*. Retrieved from reuters.com.

Straits Times. (2024, February 20). Election watchdog busts political deepfakes ahead of South Korea's April general election. Retrieved from https://www.straitstimes.com/asia/east-asia/election-watchdog-busts-political-deepfakes-ahead-of-south-korea-s-april-general-election

Suciu, Peter. (2023, December 15). Putin's Deepfake Doppelganger Highlights the Danger of the Technology. *Forbes*. Retrieved from www.forbes.com.

United Kingdom Parliament. (2023, September 5). *WITNESS – written evidence to House of Lords Communications and Digital Select Committee inquiry: Large language models*. Retrieved from https://committees.parliament.uk/writtenevidence/124270/pdf/

Witness. (n.d.). *Deepfakes, Synthetic Media and Generative AI*. Retrieved from https://www.gen-ai.witness.org

VACCINATING THE HOME TEAM:
WHEN PRICE IS NOT EVERYTHING

Jaspal Singh Sandhu, Joshua Wong Shiu Hong, Alvin Chong Shi Heng,
Kee Mui Hoon & Ng Yih Yng
Ministry of Home Affairs, Singapore Police Force & Tan Tock Seng Hospital, Singapore

ABSTRACT

The unprecedented scale and unpredictable nature of the COVID-19 pandemic led to significant procurement challenges in the healthcare supply chain. The pandemic severely tested existing preparedness plans and the whole-of-government response to an ever-evolving threat. This article shares the various challenges that the Home Team Medical Services Division had to overcome through stakeholder engagement and strategic purchasing to ramp up its vaccination programme in the face of global shortages and supplier opportunism. Using lessons learned from a proof-of-concept field deployment of a pharmaceutical grade refrigerator, the Home Team Medical Services Division was able to quickly increase and enhance the vaccine storage capabilities across all medical centres in the Home Team, in time for the roll-out of the first batch of COVID -19 vaccinations for Home Team officers involved in frontline operations.

VACCINATION POLICY FOR HOME TEAM OFFICERS

Officers of the Home Team (i.e. departments under the Ministry of Home Affairs, Singapore) have an increased risk of contracting infectious diseases given the public facing nature of their work and where available, vaccination against certain infectious diseases is one of the pivotal public health strategies in disease prevention and control, providing a safe and effective form of protection for the recipient. One of the first key goals when Home Team Medical Services Division (HTMSD) was set up in 2017 was to introduce a policy to standardise and level up vaccination practices across the Home Team. This is to safeguard the health of all Home Team officers during peacetime and to ensure an operationally ready Home Team. To further strengthen this policy, amendments were made to the relevant legislation, such as the Police Force Act and Civil Defence Act, to mandate vaccinations as part of the medical force protection for officers whose line of duty or vocation carries a higher risk of exposure (e.g., rabies vaccination for dog handlers).

The Home Team's operational vaccination programme is largely aligned with the Singapore Armed Forces (SAF)'s programme and recommendations of the national expert committee on vaccination, and adjusted based on the Home Team's operating context and exposure risk. Uniformed officers, trainees and national servicemen are given the required vaccinations at medical centres located at the Civil Defence Academy (CDA), Home Team Academy (HTA) and Gurkha Contingent (GC). Additionally, the Singapore Civil Defence Force headquarters (HQ SCDF) medical centre is the designated travel medicine and overseas vaccination medical centre that supports mission-critical inoculation for Home Team officers prior to overseas travel, training, or deployment.

Vaccines are temperature sensitive biological products and as with any vaccination programme, quality-assured cold chain maintenance is critical, and in compliance with industry standards for vaccine storage to achieve vaccine effectiveness and tolerability. However, the key pain point with a price-based approach to healthcare procurement – fiscal prudence being the hallmark of public sector integrity – is that it does not adequately address the

less tangible aspects of patient care such as quality control or the complex logistics coordination and redundancy involved in guaranteeing an unbroken cold chain transport of temperature sensitive vaccines. This challenge is especially more pronounced when dealing with large quantities of vaccines required, since the objective of the Home Team vaccination policy is to ensure adequate protection for a high throughput of personnel.

A broken cold chain, if **recognised**, may lead to the loss of thousands of vaccine doses and disruption of medical services, and if **unrecognised**, lead to the loss of medical protection, resulting in the use of non-viable vaccines and higher risk of diseases such as COVID-19 or influenza.

TAKING A STRATEGIC APPROACH TO HEALTHCARE SUPPLY

Needs Analysis

It is critical to prevent loss of vaccine potency when storing and handling vaccines (Centers for Disease Control and Prevention, 2023), especially since newer vaccines introduced tend to be expensive (Gazmararian et al., 2002).

However, the Home Team's medical centres were equipped with domestic household refrigerators for vaccine storage when they were set up between 1999 and 2006. They initially functioned like a family physician or general practitioner clinic, as compared to the primary care medical centre that now supports Home Team officers in training and operations. As most family physician/general practitioner clinics require prior appointments for vaccinations instead of walk-ins, the operating model to minimise any wastage is on-demand ordering, with the domestic household refrigerators temporarily storing these vaccines until it is ready to be administered. Hence, equipping the medical centres back then with domestic household refrigerators was seen as acceptable as the risks were manageable especially with a very low throughput of officers requiring vaccinations. However, the need for healthcare within the Home Team has grown over the last 20 years, in tandem with the nation's demographic transition to a first world, ageing population, which has led to heightened expectations of healthcare. New challenges such as infectious disease epidemics, and constant spectre of Chemical, Biological, Radiological and Explosive (CBRE) threats highlight the need for medical surge capacity that the Home Team medical centres have had to adapt to.

There is, however, an inherent risk of temperature fluctuations from household refrigerators as they are not purpose-built for temperature sensitive biological products like vaccines. Temperature fluctuations can occur without warning and not be easily or immediately detected. The non-optimal design of these refrigerators can lead to temperature stratification and the increasing wear and tear of the refrigerators as they age. When the power tripped at HQ SCDF medical centre during maintenance works on the building one weekend in 2015, the rapid warming up of the refrigerator then in place meant some S$5,000 worth of vaccines had to be disposed of. In 2016, the domestic household refrigerator in CDA broke down, forcing medical centre staff scrambling to transport vaccines to the nearest medical centre (i.e. the HTA medical centre) as a stopgap measure. While no vaccines were disposed of during this incident, there was the risk of potency of the vaccines diminishing because of the movements between the two medical centres with less than optimum cold chain management.

With the implementation of the Home Team's vaccination policy from 1 July 2018, there was a need to increase the capacity of the refrigerators for vaccine storage and to manage the high throughput of officers receiving them. A variety of vaccines including influenza, hepatitis A and B, varicella, and tetanus, diphtheria and pertussis (Tdap) have to be administered to officers and trainees across the four medical centres at a total cost of approximately S$800,000 each year. However, the domestic household refrigerators then in use at the four medical centres lacked an alarm or a system capable of triggering alerts in the event of a power trip, if the refrigerator doors were left open or ajar, or if the temperature fell outside the range of 2 to 8 degrees Celsius. Medical centre staff would have to conduct manual checks on the vaccine inventory and implement a rudimentary temperature monitoring procedure as part of their daily routine.

Furthermore, while the medical centres at HTA, Civil Defence Academy and Gurkha Contingent were then manned round the clock, HQ SCDF medical centre was not manned after office hours, during weekends and public holidays. Hence, there was a pressing need for a refrigerator that had the capability to trigger alerts remotely (via Short Messaging Service) in-situ, with an inbuilt emergency power supply or integrated with an external Uninterruptible Power Supply System that can last at least two hours during a power trip to give sufficient response time for medical centre staff to attend to any incident onsite.

Despite the clear need for pharmaceutical refrigerators, HTMSD still had to justify the viability of such a purchase. A project team comprising staff from HTMSD, Parkway Shenton Pte Ltd (Home Team's appointed medical service provider) and Home Team Science and Technology Agency (HTX) Central Procurement Office was thus set up in July 2019 to conduct the needs assessment, study industry benchmarks, engage with stakeholders and make recommendations.

Industry Benchmarks

The majority of vaccines purchased by HTMSD are required to be stored within specific temperatures ranging between 2 to 8 degrees Celsius. Prolonged periods above or below these thresholds will result in their effectiveness being reduced exponentially (Bell et al., 2001; Gazmararian et al., 2002). Guidelines from the United States Centers for Disease Control and Prevention (CDC) require that an effective cold chain contain three main elements: (i) well-trained staff, (ii) reliable storage and adequate temperature monitoring equipment, and (iii) accurate vaccine inventory management.

A study in 2009 by the National Institute of Standards and Technology (NIST), an agency of the United States Department of Commerce, tested the performance of two types of refrigerators of similar capacity – a household type dual-zone refrigerator/freezer and a pharmaceutical grade refrigerator. The objective was to determine proper storage/location within the refrigerators, temperature monitoring methods, and the effects of intermittent and continuous door opening and simulated power outages (Chojnacky, 2009). The study concluded that there are risks in storing vaccines in domestic household refrigerators as: (i) they do not maintain reliable and stable temperatures since such refrigerators lack "fan forced" cooling systems, and (ii) often have poor temperature recovery after the opening of the door (Chojnacky, 2009). Another functional issue when storing vaccines in a domestic household refrigerator is the uneven temperature distribution and temperature fluctuation from the location of the evaporator fan. This is why hospitals and polyclinics rely on pharmaceutical refrigerators as they deliver stable, reliable temperature control for clinical and pharmaceutical drug storage.

A pharmaceutical refrigerator generally has an accounting lifespan of eight years based on the Singapore Government's Instruction Manual on depreciation periods for fixed assets. To ensure that the pharmaceutical refrigerator remains operational throughout its lifespan, annual Preventive Maintenance (PM) is required and is factored in upfront as part of the purchase. The industry norm is that suppliers will package the PM with unlimited breakdown calls. This means that subsequent service calls and the labour costs incurred due to breakdown of equipment during the PM contract period will not be chargeable, with only parts or components beyond the warranty period charged as part of the ad-hoc corrective maintenance. The project team recommended a PM instead of a Comprehensive Maintenance (CM) schedule (which comprises repairs and spare parts replacement for breakdowns on top of the PM package). As these pharmaceutical refrigerators are much more specialised and durable than common, mass-produced household refrigerators, the project team's assessment was that while the CM would offer peace of mind, it might not offer value for money for such a purchase over its useful lifespan.

Stakeholder Engagement

Before establishing a procurement plan, it is critical to have a good understanding of the market dynamics of the industry from which the medical equipment and devices are to be procured. However, a comprehensive market analysis can be time-consuming and resource intensive. The project team had to consider whether the sector is going

through a period of growth, decline or stagnation which can affect prices and the stages of innovation or development a product or service goes through.

At the same time, studies have shown that conducting a value-based approach in medical equipment procurement can lead to better health and greater cost-effectiveness (Prada, 2016; Rahmani et al., 2021). Ideally, healthcare procurement includes giving preference to long term efficiency and working with suppliers to identify opportunities to develop more innovative products and services (Prada, 2016). However, it is generally difficult to shift the traditional procurement focus of cost savings to a more holistic objective comprising health system performance and patient outcomes (Rahmani et al., 2021), as the latter is not quantifiable. The diversity of stakeholders within the Home Team's procurement process (HTMSD, Home Team's appointed medical service provider, the supplier and the HTX's Central Procurement Office) makes it an uphill task to get collective buy-in and value creation.

Since true leaders do not make plans and decisions in silos, but make an effort to reach out to stakeholders for their perspectives in planning and supporting efforts (VanVactor, 2011), the project team changed its strategy to accommodate the differing views of the stakeholders.

Singapore Government's Procurement Principles

The Singapore Government adopts the fundamental principles of transparency, open and fair competition, and value for money for its government procurement policies so as to maintain probity and public trust in procurement (Ministry of Finance, 2024). Procurement policies and procedures within the Home Team are tailored based on the government procurement procedures set out in the Government Instruction Manual (IM). Within the Home Team, procurement needs cover a wide range of requirements, from simple off-the-shelf buys to complex development and systems integration projects. Hence, the Home Team subscribes to an open and transparent procurement system where the procurement objectives, criteria and procedures are made known to suppliers as far as possible. All suppliers are treated equally in a fair and transparent manner and have fair access to information on procurement opportunities and results.

Given the limited budgetary resources available to the Home Team, ensuring value for money is key to ensuring optimum utilisation of budgetary resources. Value for money can sometimes be manifested as lower costs, but it can also mean better quality of goods and services. Hence when developing the evaluation criteria, the project team worked with its stakeholders to derive an optimal balance of benefits and costs of purchasing a pharmaceutical refrigerator over a domestic household refrigerator, taking into account factors such as suitability for the intended purpose from a medical perspective, quality and reliability of the goods and service, after-sales service and support and total cost of ownership to ensure public monies are spent prudently.

Project Team's Procurement Strategy

The procurement was redesigned as a pilot to field test pharmaceutical refrigeration with the potential to scale up. Planning by the project team for the procurement of one pharmaceutical refrigerator with an Uninterruptible Power Supply System began in August 2019 and approval for the purchase was obtained in October 2019, with the delivery in November 2019. This was pitched as enhancing medical centre operations by improving the logistics and storage of expensive vaccines. Additionally, the medical centre staff no longer had to do the onerous routine of frequent manual temperature logging and conducting daily checks on the refrigerators. HQ SCDF medical centre was selected for the pilot since: (i) it was unmanned after office hours, during weekends and public holidays; and (ii) it was the designated overseas deployment for Home Team personnel, storing vaccines for personnel such as SCDF's Operation Lionheart contingent. With the overall cost of purchasing and maintaining a pharmaceutical refrigerator at almost 11 times more than a domestic household refrigerator of a similar capacity (approximately S$17,000 compared to S$1,500), it had to be justified as a worthy long-term investment. The project team had to show that the pharmaceutical refrigerator would in the long run provide cost-savings in terms of its ability to preserve sensitive biological materials because it could trigger alerts to medical centre staff.

A successful pilot would lay the groundwork for HTMSD to gradually roll out this enhancement to the

remaining medical centres. It would be less costly to scale up and procure additional units for the remaining medical centres, as well as avoiding wastage due to the disposal and replacement of degraded vaccines because of storage at out-of-range temperatures. Furthermore, the pharmaceutical refrigerators are integral to the cold chain management of the vaccines, as they allow mass storage of vaccines as part of the Home Team's health protection policy for our frontline officers, who are at a higher risk of exposure to infectious diseases during the course of work and for Home Team Departments to maintain operational readiness as well as business continuity.

ROLLING OUT THE COVID-19 VACCINATIONS

The timing of the field pilot proved to be fortuitous, as it provided proof of concept when HTMSD had to roll out the mass vaccination of Home Team officers in the midst of a global pandemic. The delivery of the pharmaceutical refrigerator came before the outbreak in Wuhan, China, in December 2019, and thus allowed the field testing to be done from November 2019 to November 2020, before the first batch of COVID-19 vaccines was made available. While the total cost of scaling up and purchasing additional pharmaceutical refrigerators was not a significant expense, there was potential for reputational damage especially since Home Team officers had been prioritised to receive the first tranche of COVID-19 vaccines and failure to coordinate and implement a successful and smooth vaccination drive could dent public confidence in the Government's rollout of the COVID-19 vaccines nationally to the general population.

During an outbreak or a pandemic, Home Team officers are at the forefront of emergency responses. Of paramount concern is ensuring officers do not succumb to an infectious or toxic agent as inadequate manning would be detrimental to the Home Team's capacity to respond to incidents and maintain public order. Hence, Home Team officers should be given the necessary protection through vaccination where applicable and preferably before deployment as vaccinations require a lead time prior to the exposure to stimulate the individual's immune system to develop specific immunity to the disease. A further consideration is that going forward, there may be other new vaccines which may be assessed to be necessary for medical protection. The challenge is to make it possible to ramp up the capability of the Home Team's medical centres at short notice with limited medical manpower.

In response to the COVID-19 pandemic, two vaccines were identified as the most effective and approved for emergency use from November 2020. Both were made by Moderna and Pfizer-BioNTech from genetic material in the form of messenger ribonucleic acid (mRNA) (Chew, 2020). The Singapore Government's plan was to begin administering the vaccines from 30 December 2020 (Health, 2020). As the initial stocks allocated were very limited, priority for vaccination would go to those at greater risk nationally, including Home Team frontline personnel.

In anticipation of the mass vaccination rollout with the arrival of the first shipment of vaccines at the end of 2020, HTMSD was tasked with the responsibility of vaccinating Home Team officers as quickly as possible. HTMSD's planned procurement of pharmaceutical refrigerators, originally scheduled for November 2022, was brought forward and expedited. Despite the short lead time given, HTMSD rallied the relevant stakeholders together to enable the ramping up of vaccination operations, ranging from the setting up of mass vaccination centres, getting the infrastructure ready, bringing in additional manpower, scheduling the vaccination slots, creating a vaccination registry and linking it up with the national system, and ensuring that vaccine storage capabilities at all four Home Team medical centres were ready.

In particular, the provision of COVID-19 vaccinations required careful and meticulous logistics coordination as compared to the norm. The mRNA-based vaccines for COVID-19 brought out a different set of challenges due to their novel development compared to other vaccines and the strict protocols (see Figure 1) they must adhere to, including ultra-low temperature storage. While mRNA-based vaccines can be produced faster than traditional vaccines, they must be stored at very low temperatures because mRNA is easily destroyed. Drug manufacturers have coated the modified mRNA in lipid nanoparticles, but it still needs to be frozen (Uddin & Roni, 2021). Pfizer's vaccine has to be stored at -70 degrees Celsius and lasts for only five days at standard refrigerator temperatures (Chew, 2020; Uddin & Roni, 2021). Moderna's

vaccine can be stored at -20 degrees Celsius and lasts in a fridge for 30 days (Chew, 2020; Uddin & Roni, 2021). Once thawed, these vaccines have a very short shelf life that ranges from five days to 30 days, depending on the manufacturer. Hence, to minimise any potential wastage, reduced efficacy of the vaccines or the possibility of adverse events arising from improper storage of vaccines when administered to Home Team personnel, extra precautions have to be taken to ensure optimum storage conditions are met (Alam et al., 2021). For a successful vaccination programme, there is a need to strictly comply with the cold chain process during manufacturing, transportation, and distribution of the vaccines to the vaccination sites (see Figure 2).

Vaccination providers are required to adhere to strict cold chain protocols to preserve the integrity of the vaccines during transport

1. Storage

a. The COVID-19 Vaccine Vials are stored in cold chain box with ice packs during transport. Temperature of the vials should be within 2ºC to 8ºC.

b. Cold chain box used must be validated before first use to ensure cold chain can be maintained throughout and detailed steps on the preparation of the cold chain box for use to be clearly written in SOP. Training is to be conducted for personnel preparing the cold chain box.

c. Vaccine vial should be securely packed with adequate protection to avoid direct contact with ice packs as well as to prevent any movement or breakages during transportation.

2. Temperature Surveillance

a. Delivery arrangements are to be equipped with real time digital thermometers with probes extending to the interior of the compartment. Additionally, there are monitors with both upper and lower limit audible alarm triggers to alert when the temperature goes out of the required range.

3. Inspection

a. Upon delivery at the vaccination site, undiluted vials are stored in the refrigerator at 2ºC to 8ºC. The temperature log is reviewed upon receiving at the vaccination site and flag out any anomalies to Vaccination Operations Task Group immediately.

Figure 1. MOH Cold Chain Protocol for COVID-19 Vaccine

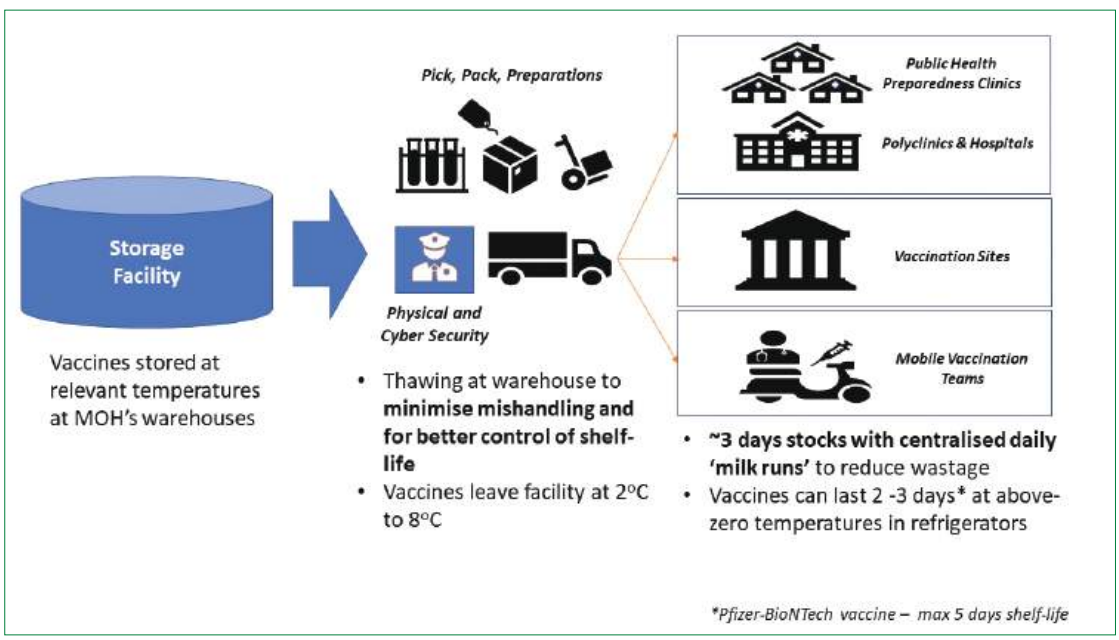


Figure 2. Cold Chain Workflow for Indenting COVID-19 Vaccine

Through establishing a good rapport with the supplier from the successful field testing of the pharmaceutical refrigerator with an Uninterruptible Power Supply System at HQ SCDF medical centre, the project team was able to act quickly to secure an additional six pharmaceutical refrigerators at the same cost for the three remaining medical centres at Civil Defence Academy, HTA and Gurkha Contingent, as well as Singapore Prison Service's Changi Medical Complex to support their vaccination programme for inmates. This was done through a fast-track procurement via direct contracting with the support of HTX Central Procurement Office. HTMSD had reached out to the three suppliers that previously participated and had met the technical requirements in the open invitation to quote as part of the pilot, but out of the three, only the incumbent supplier was able to commit to a shorter lead-time (two weeks) at the same price as compared to the other two suppliers, who indicated a longer delivery lead-time of ten to twelve weeks at increased prices. Furthermore, the two suppliers were unable to provide confirmation that they had existing stocks to meet MHA's urgent needs due to the significant demand locally for pharmaceutical refrigerators from the private and public healthcare sectors for the COVID-19 vaccination exercise. This came at a time when there was a global shortage of pharmaceutical refrigerators (Bostock, 2020; O'Donnell, 2020), leading to price gouging.

CONCLUSION

Healthcare supply chain management requires specialised expertise as it directly correlates to the resiliency of any healthcare organisation during disaster scenarios. A well-developed contingency plan hinges on a healthcare organisation being well-equipped, or risk exposing itself to abruptly halting its healthcare operations if there are no effective mechanisms available to sustain its operations. The unprecedented nature of COVID-19 pandemic severely tested global healthcare systems, exposing deficits in crisis communication, leadership, preparedness, and adaptability. The pandemic severely disrupted supply chains and the usual process in procuring goods and services as compared during normal times. While establishing the real need is the starting point of any procurement process, proactively identifying and budgeting to field test a pharmaceutical refrigerator based on enhancing medical centre operations helped to build the foundation of the concept of operations when there was a sudden need to scale up. This endeavour primed our stakeholders to have a better appreciation of the medical considerations and complexities involved in the provision of vaccinations during peacetime that cannot be addressed by the conventional procurement approach. Engaging stakeholders from the onset and explaining the efficiency and effectiveness of the product or service should be the main goal instead of potential cost savings alone. It also gave HTMSD an edge in navigating potential supplier opportunism, especially when the litmus test came in the form of the COVID-19 pandemic, which exposed the imbalance of supply and demand and disruptions in the supply chain. That edge allowed HTMSD to provide the needed protection against COVID-19 for Home Team officers throughout the course of the pandemic, minimising operational disruptions due to prolonged illness or disability due to the lack of vaccinations.

ABOUT THE AUTHORS

Jaspal Singh
was a Senior Manager in the Home Team Medical Services Division (HTMSD) of the Ministry of Home Affairs (MHA) at the time when the COVID-19 outbreak began. He previously managed healthcare procurement to ensure that organisational requirements are catered for and contracts to support MHA's long term medical and operational healthcare goals. This included strategic oversight of all the outsourced medical services at the Home Team medical centres and supporting the Home Team's response to COVID-19. He is currently an Assistant Director in the National Services Directorate in the Human Resources Division, MHA. He holds a master's degree in public health, specialising in health policy and services, from the Saw Swee Hock School of Public Health at the National University of Singapore and a bachelor's degree in medical science (Hons) from the Australian National University.

Alvin Chong Shi Heng
is an Assistant Director with the Home Team Medical Services Division (HTMSD) of the Ministry of Home Affairs since 2019. He manages diverse healthcare projects, and his portfolio includes establishing contracts and introducing new capabilities to align the medical services with evolving operational needs. In response to the global COVID-19 pandemic, Alvin was an integral member of a team which developed a vaccine management system that streamlined ground processes for the HT's COVID-19 vaccination operation. He holds a bachelor's degree in engineering (bioengineering) (honours) from the Nanyang Technological University.

Kee Mui Hoon
was a Deputy Director in the Home Team Medical Services Division (HTMSD) of the Ministry of Home Affairs, Singapore. She provided oversight on the Home Team medical centres operations and healthcare procurements to support frontline operational readiness. During the COVID-19 pandemic, she led her team to plan, coordinate and operationalise various COVID-19 operational requirements such as ensuring pandemic preparedness of the HT medical centres, set up the Home Team COVID-19 vaccinations centres and support Home Team departments in ad-hoc and urgent mass swab testing beyond mandatory requirements for additional surveillance purposes. She is currently Deputy Director in the Administrative and Finance Department in the Singapore Police Force. She has a bachelor's degree in business from the Nanyang Technological University.

Joshua Wong Shiu Hong
joined the Ministry of Home Affairs, Singapore in 2017 as the Director of the Home Team Medical Services Division (HTMSD). He currently serves as a Medical Consultant in HTMSD, providing oversight on matters pertaining on occupational health such as developing the Home Team Occupational Health Registry, analysis of occupation related costs, case data and health trends and formulating operational health requirements to support Home Team departments' operations. He specialises in preventive medicine and is an occupational medicine specialist, and concurrently practices at Sengkang General Hospital. He completed his medical education and earned a master of public health degree at the National University of Singapore.

Ng Yih Yng
is the Director of the Digital and Smart Health Office, Centre for Health Innovation, National Healthcare Group focused on innovation, digital health and Artificial Intelligence (AI). He is trained as an emergency and public health specialist and is a senior consultant at the TTSH Department of Preventive and Population Medicine. He previously served as the Home Team Chief Medical Officer, Ministry of Home Affairs and oversaw healthcare policies across the Home Team departments. He is the Clinical Director of the World Health Organisation Collaborating Centre for Digital Health and Health Education at the Lee Kong Chian School of Medicine, and an implementation lead at the NTU Centre for AI Medicine (C-AIM). He graduated as a medical doctor at National University of Singapore, an emergency physician from the Royal College of Surgeons (Edinburgh), earned Masters of Public Health and Business Administration degrees from Johns Hopkins University and a Masters of Technology (Digital Leadership) at NUS-Institute of System Science during COVID.

REFERENCES

Alam, S. T., Ahmed, S., Ali, S. M., Sarker, S., Kabir, G., & Ul-Islam, A. (2021). Challenges to COVID-19 vaccine supply chain: Implications for sustainable development goals. *International Journal of Production Economics, 239*, 108193. doi:10.1016/j.ijpe.2021.108193

Bell, K. N., Hogue, C. J., Manning, C., & Kendal, A. P. (2001). Risk factors for improper vaccine storage and handling in private provider offices. *Pediatrics, 107*(6), E100. doi:10.1542/peds.107.6.e100

Bostock, B. (2020, 19 October). 3 billion people could struggle to get a COVID-19 vaccine because the world doesn't have enough fridges to store it. *Business Insider*. Retrieved from https://www.businessinsider.com/coronavirus-vaccine-world-fridge-shortage-delay-rollout-affect-world-poorest-2020-10

Centres for Disease Control and Prevention. (2023). *Vaccine Storage and Handling Toolkit*. United States: Centers for Disease Control and Prevention Retrieved from https://www.cdc.gov/vaccines/hcp/admin/storage/toolkit/index.html

Chew, H. M. (2020, 23 December). How COVID-19 vaccines are transported to Singapore and stored here *Channel NewsAsia*. Retrieved from https://www.channelnewsasia.com/singapore/covid19-vaccines-cold-chain-changi-transport-singapore-pfizer-501086

Chojnacky, M., Miller, W., Ripple, D., & Strouse, G. (2009). *Thermal Analysis of Refrigeration Systems Used for Vaccine Storage: Report on Pharmaceutical Grade Refrigerator and Household Refrigerator/Freezer*. NIST Interagency/Internal Report (NISTIR) Retrieved from https://www.nist.gov/system/files/documents/2017/05/09/NISTIR7656-Thermal-Analysis-of-Dorm-style-Refrigerator-and-Freezerless-Refrigerator-for-Vaccine-Storage.pdf

Gazmararian, J. A., Oster, N. V., Green, D. C., Schuessler, L., Howell, K., Davis, J., . . . Warburton, S. W. (2002). Vaccine storage practices in primary care physician offices: assessment and intervention. *American Journal of Preventive Medicine, 23*(4), 246-253. doi:10.1016/s0749-3797(02)00512-3

Health, M. o. (2020). Expert Committee Submits Recommendations On Singapore's Covid-19 Vaccination Strategy. Retrieved from https://www.moh.gov.sg/news-highlights/details/expert-committee-submits-recommendations-on-singapore-s-covid-19-vaccination-strategy

Health Sciences Authority. (2021). HSA Approves New Storage Condition for the Pfizer-Biontech Covid-19 Vaccine at Refrigerator Temperature for up to 31 Days [Press release]. Retrieved from https://www.hsa.gov.sg/announcements/press-release/pfizervaccine-refrigeratortemp31days

Ministry of Finance. (2024). Government Procurement Guide for Suppliers. Retrieved from https://www.gebiz.gov.sg/docs/Supplier_Guide_Detailed.pdf

O'Donnell, C. (2020, 10 November). Why Pfizer's ultra-cold COVID-19 vaccine will not be at the local pharmacy any time soon. *Reuters*. Retrieved from https://www.reuters.com/article/health-coronavirus-vaccines-distribution-idUSKBN27P2VP

Prada, G. (2016). Value-based procurement: Canada's healthcare imperative. *Healthcare Management Forum, 29*(4), 162-164. doi:10.1177/0840470416646119

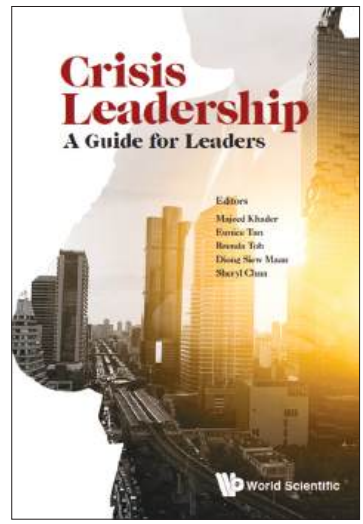
Rahmani, K., Karimi, S., Rezayatmand, R., & Raeisi, A. R. (2021). Value-Based procurement for medical devices: A scoping review. *Medical Journal of The Islamic Republic of Iran 35*, 134. doi:10.47176/mjiri.35.134

Uddin, M. N., & Roni, M. A. (2021). Challenges of Storage and Stability of mRNA-Based COVID-19 Vaccines. *Vaccines, 9*(9). doi:10.3390/vaccines9091033

VanVactor, J. D. (2011). Cognizant healthcare logistics management: ensuring resilience during crisis. *International Journal of Disaster Resilience in the Built Environment, 2*(3), 245-255. doi:10.1108/17595901111167114

RECENT PUBLICATIONS BY HOME TEAM STAFF

BOOKS



Crisis Leadership: A Guide for Leaders

By Majeed Khader, Eunice Tan, Brenda Toh, Diong Siew Maan and Sheryl Chua
Published by World Scientific, May 2023, 244 pages

In the context of our world increasingly characterised by volatility, uncertainty, complexity and ambiguity, and with the proliferation of modern crises, crisis management has evolved into a key task area that is no longer critical only to the energy, aviation, and security sectors and neither is it only the work of appointed crisis managers. Beyond the traditional acute crises, there are creeping crises, looming crises and black swan events, and also crises that have multiple, differentiated and non-linear trajectories. What then are the structures and capabilities necessary for organisations and leaders to be prepared to face this diverse range of modern crisis situations?

The book presents several key competencies that crisis leaders and managers should possess and develop for effective crisis management. For instance, leaders would have to possess digital and cross-cultural competence, embody adaptive authenticity, manage tasks, engage in collective sensemaking, display transformative and agile leadership, and manage misinformation. The genesis of the qualities entailed a literature review, opinion surveys administered to officers who manage crises in their roles, and interviews with leaders and incident managers, as well as discussions with subject matter experts on the topic of Crisis Leadership. This book offers practitioners a better understanding of essential crisis leadership qualities and practical recommendations for action and development.

Beyond the crisis leader, this book highlights the importance of the crisis-ready organisation and network. The interplay between the crisis leader and the broader organisational and operating systems in shaping effective crisis management is discussed, with implications for leaders and organisations in developing and enhancing the crisis ecosystem so that crises can be effectively prevented, managed and learned from.

Majeed Khader, Diong Siew Maan and Eunice Tan are with the Home Team Psychology Division, formerly the Home Team Behavioural Sciences Centre (HTBSC). Brenda Toh was formerly with HTBSC and Sheryl Chua is with the Singapore University of Social Sciences.

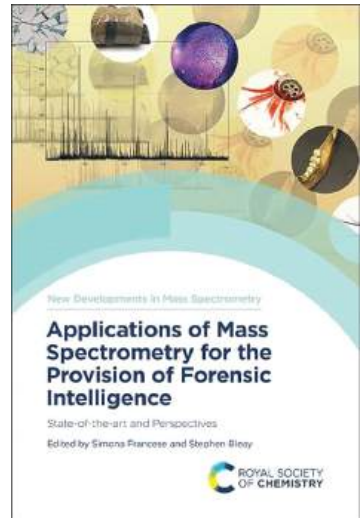
Chapter 1 – Applications of Mass Spectrometry to Explosive Casework: Opportunities and Challenges

By Goh Ho Wee and Fang Guihua

In *Applications of Mass Spectrometry for the Provision of Forensic Intelligence*

Edited by Simona Francese; Stephen Bleay

Published by Royal Society of Chemistry, 2023, 322 pages



Mass spectrometry is an essential technique employed in forensic investigations to identify trace explosive materials and is increasingly relied upon to analyse larger samples for the provision of forensic intelligence. Only in an operational setting are forensic intelligence efforts truly realised, and it is through this lens that readers and researchers must focus their efforts. This chapter outlines current and emerging techniques used in operational forensic laboratories in Australia, Canada, Singapore and the US, providing case studies as exemplars. Importantly, the challenges and limitations of such work are discussed, as well as opportunities moving forward.

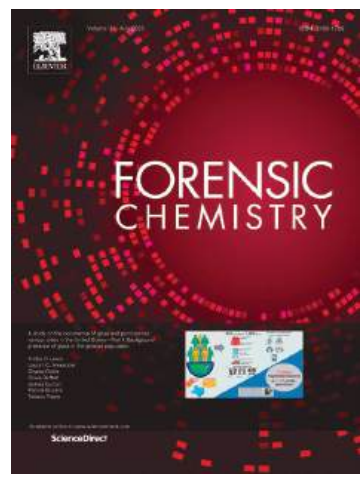
Goh Ho Wee is a Deputy Director in the CBRNE Centre of Expertise of the Home Team Science & Technology Agency. Fang Guihua is a Senior Forensic Scientist in the Forensic Chemistry & Physics Laboratory of Health Sciences Authority.

JOURNAL ARTICLES

Screening Unknown Novel Psychoactive Substances using GC-MS based Machine Learning

By Wong Swee Liang, Ng Li Teng, Justin Tan, Jonathan Pan

In Forensic Chemistry, Volume 34
Elsevier, July 2023



Recent years have seen a large increase in structural diversity of novel psychoactive substances (NPS), exacerbating drug abuse issues as these variants evade classical detection methods such as spectral library matching. To address this issue, the Home Team Science & Technology Agency developed an AI classifier to predict if an unknown substance (even those which have not yet been recorded/ encountered) belongs to one of the six different NPS drug classes: cathinone, cannabinoids, phenethylamine, piperazine, tryptamines and fentanyl. This development has the potential to speed up the identification of unknown NPSes, and the decision-making process for our officers encountering such substances at our borders and drug-related crime scenes.

All authors are from the Home Team Science & Technology Agency. Justin Tan is a Forensic Scientist, Ng Li Teng is a CBRNE Scientist, and Wong Swee Liang and Jonathan Pan are from the Disruptive Technologies Office.

THE HOME TEAM COMPRISES 11 AGENCIES:

Ministry of Home Affairs Headquarters • Singapore Police Force • Internal Security Department • Singapore Civil Defence Force • Immigration & Checkpoints Authority • Singapore Prison Service • Central Narcotics Bureau • Home Team Academy • Home Team Science and Technology Agency • Gambling Regulatory Authority • Yellow Ribbon Singapore

All Home Team departments and agencies work together as one, in close partnership with the community, to keep Singapore safe and secure.

The Home Team Academy's mission is to empower learning and growth, and enable a united and successful Home Team. It aspires to be a leading corporate university in homefront safety and security.

www.mha.gov.sg/hta

ISSN: 2010-0617