

HOME TEAM JOURNAL

Issue
no. **12**
February 2023

by Practitioners, for Practitioners

EMERGING THREATS

- Crime & Technology:
Crypto-Assets, the Metaverse,
Encrypted Communications,
Cyber Sextortion
- Illicit Drugs
- Youth Radicalisation

T. RAJA KUMAR

on Singapore's Presidency of the
Financial Action Task Force:

"The scale of online cyber-crime is staggering. This is why I have made strengthening asset recovery through effective and meaningful international cooperation one of the key priorities of my FATF presidency."

SPECIAL FEATURE ON SCAMS

How to protect your loved ones from scams

The BSC Brief

Deception Detection across Cultures

THE LEADERSHIP INTERVIEW

"At the end of the day, leadership is about bringing people together to get the job done. And in order to do that, you must be able to communicate, persuade and convince people why they should do the things you say is important, including giving people a sense of purpose, giving them a sense of mission."

MARVIN SIM

Commissioner of Immigration &
Checkpoints Authority



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.

PUBLISHER

Home Team Academy

ADVISORS

Anwar Abdullah

Chief Executive, Home Team Academy

Teo Tze Fang

Deputy Chief Executive, Home Team Academy

PROJECT DIRECTOR

Winston Wong Sung-En

Director, Centre for Planning,
Technology & Communications,
Home Team Academy

EDITOR

Susan Sim

MANAGING EDITOR

Tan Puay Seng

ASSISTANT MANAGING EDITORS

Melissa Teh

Zainab Mohamed Arkam

COPY EDITOR

Lim Jing Jing

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

Ee Kiam Keong
Gambling Regulatory Authority

Chen Yeang Tat
Home Team Science & Technology Agency

Majeed Khader
Chief Psychologist, Ministry of Home Affairs

Lal Nelson
Research & Statistics Division, Ministry of Home Affairs

Lee Fook Kay
Chief Scientist, 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

Tricia Ortega
Training & Competency Development Division,
Ministry of Home Affairs

Daniel Tan
Singapore Prison Service

Teong How Hwa
Singapore Civil Defence Force

CONTENTS

Issue no.12 - February 2023

FOREWORD

03 **by Anwar Abdullah,
Chief Executive,
Home Team Academy**

THE LEADERSHIP INTERVIEW

05 **with Marvin Sim, Commissioner of
Immigration & Checkpoints Authority**
Susan Sim
Editor, *Home Team Journal*

PREPARING FOR EMERGING THREATS

23 **FINANCIAL CRIMES
SINGAPORE'S
PRESIDENCY OF
THE FINANCIAL
ACTION TASK FORCE:
FIGHTING FRAUD AND
TRANSNATIONAL CRIME
MORE EFFECTIVELY**
T. Raja Kumar
President, Financial Action Task Force

30 **ORGANISED CRIME
COMMUNICATIONS
INFILTRATING
ENCRYPTED CRIMINAL
COMMUNICATIONS: THE
AUSTRALIAN FEDERAL
POLICE'S OPERATION
IRONSIDE**
Nigel Ryan
Australian Federal Police

35 **TECHNOLOGY-
FACILITATED CRIMES
THE EMERGING THREAT
OF SEXUAL VIOLENCE IN
THE METAVERSE**
Karthigan Subramaniam &
Kwek Boon Siang
Home Team Psychology Division,
Ministry of Home Affairs, Singapore

46 **CYBER SEXTORTION:
WHO'S REALLY BEHIND
THE WEBCAM?**
Tan Wei Liang, Carolyn Misir &
Jansen Ang
Police Psychological Services
Department, Singapore Police
Force

63 **TERRORISM
TOWARDS A YOUTH-
CENTRIC APPROACH IN
THE REHABILITATION
OF RADICALISED
YOUTHS**
Ng Li Ling
Counter Terrorism Research Division,
Ministry of Home Affairs, Singapore

DRUG TRAFFICKING

72 **DEVELOPMENTS IN THE
ILLICIT DRUG MARKET
IN EAST AND
SOUTHEAST ASIA**
Regional Office for Southeast
Asia and the Pacific (Bangkok)
United Nations Office on Drugs and Crime

SCAMS

85 **CYBERCRIMINALS
AND COVID-19
SCAMS: COGNITIVE
VULNERABILITIES
LEADING TO SCAM
SUSCEPTIBILITY
AND VICTIMISATION,
PREVENTION AND
FUTURE DIRECTIONS**
Mkay Bonner &
Mark S. Johnson
University of Louisiana Monroe,
United States of America

100 **EXPLORING
GUARDIAN-CENTRIC
SCAM PREVENTION
ATTITUDES: HELP!
HOW DO I PROTECT MY
LOVED ONE FROM JOB
SCAMS?**
Stephanie Chan &
Amanda Tan
Home Team Psychology Division,
Ministry of Home Affairs, Singapore

CONTENTS

Issue no.12 - February 2023

ORGANISATIONAL RESILIENCE

109 THRIVE – A PSYCHOLOGICAL SUPPORT FRAMEWORK FOR SINGAPORE POLICE INVESTIGATORS

Neo Hui Fang Samantha, Alyah Dinah Zalzuli, Athena Rachel Willis, Ho Hui Fen & Jansen Ang
Police Psychological Services Department, Singapore Police Force

122 PSYCHOLOGICAL CRISIS SUPPORT THROUGH A PANDEMIC: THE ICA EXPERIENCE

Naomi Liew & Poh Li Li
Immigration & Checkpoints Authority, Singapore

135 SCDF'S EMERGENCY RESPONDERS' FITNESS CONDITIONING AND ENHANCEMENT LAB (EXCEL)

Hasan Kuddoos & Melissa Choo
Singapore Civil Defence Force

144 FACILITATING DATA ANALYTICS SKILLS ACQUISITION IN THE HOME TEAM

Tanny Ng, Rachelle He & Nicole Lee
Centre for Home Team Skills Transformation, Home Team Academy, Singapore

SOCIAL RESILIENCE

153 UNDERSTANDING ONLINE HATE SPEECH: A BEHAVIOURAL SCIENCES AND PSYCHOLOGICAL PERSPECTIVE

Hong Jingmin, Nur Aisyah Abdul Rahman, Gabriel Ong, Shamala Gopalakrishnan & Majeed Khader
Home Team Psychology Division, Ministry of Home Affairs, Singapore

HOMEFRONT INSIGHTS

169 THE BSC BRIEF DIVERSE CULTURES, DIFFERENT LIARS: INSIGHTS INTO DECEPTION DETECTION IN CROSS-CULTURAL INTERACTIONS

Stephanie Chan & Stephenie Wong
Home Team Psychology Division, Ministry of Home Affairs, Singapore

PUBLICATIONS

178 RECENT PUBLICATIONS BY HOME TEAM STAFF



Copyright © 2023. All rights reserved.

No part of this publication (content and images) may be reproduced, stored in a retrieval system, or transmitted in any form or by any means, electronic, mechanical, photocopying, scanning, recording or otherwise, without the prior written permission of the Home Team Academy.

The opinions expressed in this issue are the authors' and do not necessarily reflect those of the Home Team Academy or the authors' departments.

FOREWORD



It is often said that the price of freedom is eternal vigilance. For the Home Team, this axiom always holds true. We stand vigilant as guardians protecting Singapore against security threats. And this means constantly scanning the horizon for **emerging threats**.

In this issue, we throw the spotlight on how some security threats have been evolving and what the Home Team and its partners are doing to counter and prevent the growth of these threats.

Often, these threats have a helping hand from technology. Organised crimes have long been using technology to carry out age-old crimes like money laundering, drug trafficking and extortion. As T. Raja Kumar, the first Singaporean to be appointed President of the Financial Action Task Force, points out: crypto-assets are being used by criminals to store and move their proceeds from illegal activities. Crime syndicates communicate with each other via encrypted communications platforms, although perhaps more warily now following the Australian Federal Police's (AFP) Operation Ironside. The successful take-down of thousands of criminals around the world through the introduction of a trojan horse app to infiltrate encrypted communications is described in an article contributed by Assistant Commissioner Nigel Ryan, the AFP officer responsible for the operation.

Technology has also opened up new frontiers for criminals. Colleagues from the Home Team

Psychology Division, Karthigan Subramaniam and Kwek Boon Siang, highlight the alarming development of sexual predators prowling the metaverse to prey on women and children. They use immersive technological tools like virtual reality and haptic technology to commit sex crimes that are as traumatic for the victims as in the physical world. Even older technologies like webcams have been given new uses by crime syndicates. Tan Wei Liang, Carolyn Misir and Jansen Ang from the Singapore Police Psychological Services Department discuss how victims in Singapore are being blackmailed by cyber sextortion rackets overseas which threaten to distribute compromising sexual material unless their demands are met.

Other threats like illegal drug trafficking and terrorism have evolved such that they require continued societal resolve to mitigate their impacts. The United Nations Office on Drugs and Crime's regional office in Bangkok sounds the alarm about drug syndicates capitalising on the falling costs of production to sell more and cheaper synthetic drugs to Southeast Asian users. From the Counter-Terrorism Research Division of the Ministry of Home Affairs, Ng Li Ling reminds us that terrorist ideologies disseminated online have led to a global surge in the self-radicalisation of youths, requiring new forms of rehabilitation interventions. As terrorist groups and criminal syndicates advance, law enforcement authorities must innovate faster to stay ahead of the game.

At the same time, **scams** continue to be a problem worldwide. Professors McKay Bonner and Mark S. Johnson from the University of Louisiana Monroe of the United States of America detail how the COVID-19 pandemic has incubated a fertile environment for scammers to thrive, and Stephanie Chan and Amanda Tan from the Home Team Psychology Division provide tips on how guardians can help to protect their loved ones from falling victim to job scams.

Of course, technology is not just leveraged by terrorists and syndicates. The Home Team has been an avid and adept user of technology. Hong Jingmin and her colleagues from the Home Team Psychology Division used cutting-edge

deep learning techniques for Natural Language Processing (NLP) tasks to study 233,997 Facebook posts and responses to identify the common targets and intensities of hate speech in Singapore. The use of such data analytics will enable us to gather and analyse ground sentiments much more efficiently than through conventional techniques like polls and manual analysis.

Similarly, the Home Team **training** community has been using the latest technology to equip officers with the skills and knowledge they need to achieve mission success. The Singapore Civil Defence Force (SCDF) has been using extended reality (XR), to monitor and improve training effectiveness. Training tools such as a virtual reality firefighting training module and driving simulator are currently used to allow SCDF officers to train in a safe and controlled environment without constraints imposed by the physical environment.

Our own Home Team Academy (HTA) understands that championing digital upskilling is a crucial part of developing future-ready Home Team officers. Across the Home Team Departments, data analytics have already been used to make informed decisions and respond efficiently to incidents across various domains including policing, counter-terrorism, fire-fighting, border operations, rehabilitation, corrections and drug control. To ensure the Home Team continues to leverage data analytics, HTA has been supporting the digital transformation drive by equipping every single officer with data analytics skills.

To prepare for future threats, the Home Team also needs to continue building **organisational resilience**; the Singapore Police Force and Immigration & Checkpoints Authority (ICA) share their insights in this issue.

Indeed, the resiliency of all Home Team officers was severely tested during the COVID-19 crisis, as Commissioner Marvin Sim notes in The Leadership Interview, when his department found itself in the unfamiliar territory of administering and enforcing Stay Home Notices. He shared about the importance of communication during a crisis, during which he thoughtfully crafted and sent emails to uplift staff morale and strengthen resilience.

The best form of crisis management is preventing them from happening in the first place. This is why understanding emerging threats is so important. Our partners around the world recognise this. To this end, the Milipol Asia-Pacific conference supported by the Ministry of Home Affairs and the Ministry of the Interior of France, and the Asian Conference of Criminal & Operations Psychology organised by the Home Team Psychological Services held in 2022 were useful gathering points for like-minded practitioners to learn from each other. I hope this issue's *Journal*, too, helps our homefront security practitioners continue these conversations.

ANWAR ABDULLAH

Chief Executive, Home Team Academy

THE LEADERSHIP INTERVIEW

with **Marvin Sim**

Commissioner, Immigration & Checkpoints Authority



“As leaders we must always try to create a place whereby people want to wake up in the morning and look forward to going to work. Usually there are three things why people will want to go to work – the bosses that you have, the colleagues that you have, and the kind of work that you do. And these are three things everybody in the organisation can help to shape and make a difference because we are all bosses to somebody, we are all also colleagues to somebody and we all have a say in how we want to shape the work that we do.”

”

During his first day on the job at Immigration & Checkpoints Authority (ICA), someone told Marvin Sim that as Commissioner, he would very likely not have met every one of its 6,000 officers by the time he completed his tour of duty. So he set out to meet everyone in ICA.

Leadership is about communicating the organisation’s goals and your priorities and carrying the people with you, he tells *Home Team Journal* editor, **Susan Sim**.

ICA is a service department where “demands are all public-driven ... I cannot shape or dictate when Singaporeans want to go for holidays and leave Singapore and come back. I cannot dictate when people want to apply for Permanent Residence or Singapore Citizenship,” he notes. For ICA to be able to react efficiently to surges in public demand, it therefore has to streamline its processes and optimise limited resources “so that there’s less wastage.”

To explain policy and planning decisions and his own thinking, Commissioner Sim writes regular emails to his officers, explaining clearly the mission requirements and his expectations. He also makes it a point to assure them that so long as they do their best, no one will be penalised for making mistakes. Trust is a two-way street, he stresses.

He begins **The Leadership Interview** by noting candidly that he failed his A Levels on his first attempt because he was busy playing rugby, but then did well enough to go to the university. When he joined the Central Narcotics Bureau (CNB) as one of its first few batches of graduate officers, he thought he would stay only two years, but found himself moving from one post to another without thinking too much about his career progression. “I took on every posting without knowing what was going to happen next. If I had been asked, what people always ask at job interviews, where do you see yourself in five years’ time, I wouldn’t have been able to answer them.”

Following is an edited transcript¹ of the Journal's interview with Commissioner Sim:

TAKE THE STAFF POSTINGS; YOU DON'T PICK UP LEADERSHIP SKILLS FROM COURSES

You started your career in the public service in the Central Narcotics Bureau. And then you've had staff postings in the Ministry of Trade and Industry, also MHA headquarters. Did you at any time see yourself becoming the top border security chief in Singapore?

Definitely not at all, not at any time until I was actually told about this posting possibility in ICA because firstly, I'm not a scholar. Secondly, I failed my 'A' levels, so I spent three years – people spent two years, I spent three years – on it. So never did I at any time think that I would one day take on a head of department position in the Home Team.

In fact, when I joined back in 1996, I told myself then that I'll probably spend at most two years with CNB to experience what it is like working in a drug law enforcement job.

Let's go back. What do you mean you failed your 'A' levels? How does that happen?

I repeated my 'A' levels. The first time round, I didn't have the full 'A' level cert. I had to re-sit my 'A' levels in college. So I spent three years in a JC [junior college].

Were you in science, arts –

Commerce.

Nobody fails commerce!

Basically I didn't study. Of course, maybe in the world that you operate in, nobody fails, but in my world, there are people who fail.

Were you a pai kia [bad kid] then?

No, I just spent a lot of time playing and not attending and skipping lessons.

You were busy playing sports?

Yes. I played rugby.

You are proof then that one can fail school exams and still do very well.

Yes, although this is not the point that I bring up quite often. But definitely it shows that the system does work. It's not for me to say whether I've done very well but when I first joined CNB, I thought I would just spend two years there, but I continued on because the job was interesting, it was challenging. Then along the way I had postings, got to do different things so one thing led to another, I just stayed on.

What attracted you to CNB in the first place?

Prior to joining CNB, I'd never even heard of CNB. I was in NTU [Nanyang Technological University] and I had some time to kill before a lecture and they happened to be doing an MHA career talk for uniformed services in one of the lecture theatres, so I just went in to hear what they had to offer and that's the first time I heard about this organisation

Key Milestones

1996: Joined the Central Narcotics Bureau after graduating from the Nanyang Technological University.

2005: Obtained a Master of Science in International Political Economy from the S. Rajaratnam School of International Studies, NTU.

2009: Seconded to the Ministry of Trade & Industry as Deputy Director of Northeast Asia Division.

2011: Appointed as Deputy Director of the Central Narcotics Bureau.

2015: Appointed as Senior Director of the Joint Operations Group in the Ministry of Home Affairs.

2018: Completed the Stanford Executive Programme at Stanford University.

September 2018: Appointed as Commissioner of Immigration & Checkpoints Authority.

Previous key appointments: Held various leadership appointments in the Special Task Force, Investigation and Supervision Divisions of the Central Narcotics Bureau.

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

called Central Narcotics Bureau. I guess back in the 1990s – CNB was formed in 1971, but it was only when Mr Sim Poh Heng became Director in the early 90s that it started recruiting graduates for senior officer roles.

You were one of the first few graduates?

Yes, I was one of the first few graduates recruited as direct entry senior narcotics officers. Prior to that, they didn't do many such recruitments.

When I look back at my career, I took on every posting without knowing what was going to happen next. If I had been asked, what people always ask at job interviews, where do you see yourself in five years' time, I wouldn't have been able to answer them.

In fact, my attitude is: for every posting you are asked to take on, you just take it on and do it to the best of your abilities.

You joined in 1996? 1995 was when Wong Kan Seng announced the concept of the Home Team.

Yes. In 1997 when I was the OC of the Ang Mo Kio CNB team – then they called it Supervision 'F' Division – we organised Home Team sector events. I think we were one of the first sectors, together with Police 'F' Division and SCDF [Singapore Civil Defence Force], to organise a HT Sector event.

You're still a CNB officer?

Yes, I'm still in what they call the Home Team Uniformed Service (Narcotics Service). It's interesting how I ended up in MTI [Ministry of Trade and Industry] in 2009 and 2010. Around then there was one of those talent development schemes called HiPo [for high potential officers]. I was told that as part of the HiPo programme, I should do a stint out of CNB. Initially, there was some opening in MHA, so I went for an interview but I didn't get selected. Then HR [Human Resources] came back and said they checked with PSD [Public Service Division], there's another opening in MTI. They asked me whether I was interested. I said why not. I took a look at the JD [job description] – it was MTI's Northeast Asia Desk, and I had some

interest in economics, so I thought why not go and try to do something completely different. I went for an interview and MTI took me in. So that's how it all happened.

So if you look at all my postings, I would say nothing was planned too far ahead. When I took on a posting, I didn't know what I would be doing after the posting.

The larger point I want to make is that while I wouldn't say that the public service will comprehensively develop each and every one of us – which is not possible, because there's just so many of us, it's not possible to develop tailored plans for everybody, right? But there's also no lack of opportunities. At the end of the day, it is really up to the individual officer. When there is an opportunity in front of you, are you prepared to seize it?

I say this because even today, I have to convince officers sometimes to take on external postings. There're still officers who are very reluctant to try, so I have to convince them and share with them my own experiences that it's perfectly fine, just take it as doing another job with a safety net that you can eventually come back to ICA.

You can now tell them that one CNB officer went to MTI for a posting on his way to becoming Commissioner of ICA.

Yes. In fact, when I look back over my career, over twenty years, I think I benefitted the most from the MTI posting. That posting really opened up my perspective, changed how I look at things, how I look at policy development. Before that, from 1996 to 2008, I spent all my time at CNB doing drug law enforcement, never even went through a staff posting. Today, we are a bit more structured – you do ground postings, staff postings. Back then, there's no such thing as a staff posting because Mr Sim Poh Heng believed that "I hire you as a uniformed officer means you should be deployed on the ground doing law enforcement, right?" His thinking was that I pay you a premium means you go to the ground and do drug law enforcement. So when I moved over to MTI, it was my very first time dealing with issues like staffing, staff submissions. The learning curve was steep, but I benefitted, really

opened up my perspective – how to see issues, how policies are developed.

What are the differences between leading CNB, which most think of as a small Home Team department that is very mission-focused, and running one of the largest departments in the Home Team that does just about a bit of everything, that's like a microcosm of all the Home Team departments?

The key differences are in two main areas. The first is the difference in staff strength. And also because of the number of years I spent there, when I was Deputy Director, I knew almost everybody in CNB. You really get to know each and every person, some better than others, but generally you know, you have seen everybody in CNB. You can engage everyone, get a very good pulse of the organisation.

But in ICA, I still remember the first day, at one of the first events in ICA that I attended, someone told me that as Commissioner, it's highly likely that when I complete my tour, I will not have met everyone in ICA. That's the biggest difference. And so I make it a point to try to meet as many ICA officers as I can.

And the second key difference is that in CNB, you are usually in control of your operations because these are intel-driven operations, you decide when, how, what you want to hit. Even when you mount island-wide operations, you're in control.

In ICA, our demands are all public-driven. At the checkpoints, airport, services centres, I cannot shape or dictate demands for my services. I cannot shape or dictate when Singaporeans want to go for holidays and leave Singapore and come back. I cannot dictate when people want to apply for Permanent Residence or Singapore Citizenship. That's the biggest difference, because you are not in control, you can't shape the demands on you. You have to react. Then you have to organise your organisation and resources in a way that optimally you'd be able to react. So ultimately, yes, leadership skills don't differ much, but some of the things you need to do can be quite different between ICA and CNB.

In ICA, a lot is about trying to optimise your resources, organise them properly, streamline the processes so that there's less wastage, you're more efficient in meeting the public demand.

But how do you learn all that? How do you make that transition?

You can't. How should I put it? You don't attend a course and know what to do. I don't think there's such a course out there. I guess these are skills you pick up over the course of your career – for me, from my time in CNB, even in MTI, then back to CNB, and then I went to Joint Ops Group. You work with different bosses and pick up some of the skills.

For my ICA stint, what prepared me the most was my stint in JOG, as SD JOG [Senior Director Joint Operations Group] because in that portfolio, I worked quite closely with PS Leo Yip and PS Pang Kin Keong, so I could sense from their perspectives what are some of the issues across the Home Team that are important. Because I was actively coordinating a lot of the operations, processes across the Home Team, I also had a ringside seat seeing some of the issues in ICA, what are some of the things other Home Team departments are doing, which maybe ICA is not doing. So I would say the stint in JOG prepared me for this post quite well. It's in those kinds of postings, where you work for different bosses that you pick up some of these skillsets along your way. I clearly attended courses, but it is not enough.

It also sounds like staff postings are very important.

They are, they are. In fact, if you ask me – it's always quite interesting that uniformed officers, whether in CNB or ICA, from time to time, there'll be somebody who will say, "oh I'm a uniformed officer, I don't know how to do staff work." Why is it that only civilians can do staff work? Why is it only civilians who can record minutes? We all graduated from the same universities, right? Why is it that civilians who join MHA can do better staff work than uniformed officers? Sometimes I think underlying this is that it's not so much of who can write better but it's also the exposure and thinking that goes through doing staff work. And because uniformed officers are so used to running teams and responding to ground issues, running operations, over time, they are not exposed to think differently in terms of policy. Which is why I think for anyone who is being groomed for leadership positions, it's very, very important to go through staff postings. Not so much to write minutes, but really to go through the full works to better understand how policies are being developed, what are the trade-offs that you need to think

about, what are their importance. When you have to manage trade-offs, you have to prioritise what is important and what is not.

And in different portfolios, the trade-offs and prioritisation change. If you don't go through a staff posting, it's very difficult to pick up some of these instincts that you want to hone over time, over a two, three years kind of posting. Doing project works is not enough.

But doing operations work, being on the ground, that's also very important because you've got to learn how to lead people, right?

Yes. Just to make sure I get my point right – I'm not trivialising operations work. I'm just saying that because uniformed officers are so predisposed to just doing operations, when you suddenly ask them to do staff work, they find it very difficult to make the transition.

In fact, ideally to hold a leadership position, you need to be able to do both well at the same time because operations help you to lead, hone your operational instincts because sometimes the operational instinct and policy instinct are quite different. The trade-off is also quite different. The prioritisation also, because in operations sometimes you need to make decisions on the fly under quite tight timelines whereas with policy trade-offs sometimes you have a bit more time – but not that it's a much easier trade-off – you just have more time to think about some of the issues. The kind of skillsets required for both can be quite different. If you're perpetually just doing one and not the other, over time, you may find that you have lost a bit of the instinct to do either one or the other.

YOU MUST COMMUNICATE A CLEAR SENSE OF PURPOSE. AND BE AUTHENTIC

As Commissioner ICA, which skillsets do you think you use more now?

I think in any place, as leaders, communication skills are the most important. This is a function of what I believe leadership is about. To me, at the end of the day, leadership is about bringing people together to get the job done. And in order to do that, you must be able to communicate, persuade and convince people why they should do the things you say is important, including giving people a sense

of purpose, giving them a sense of mission. When there are difficult things or challenges, you must be able to communicate and explain and persuade them why this is the right thing to do, what is the right path to take.

As the head of the organisation, you cannot run away from that. So if you ask me to pick one skillset, that to me is the most important skillset. I'm not an extrovert, but it doesn't mean that I can run away from not doing these things.

For example, when I came over to ICA, in our first management retreat back in 2018, the first thing I had to do was to convince my ICA colleagues why it was important for us to embark on our transformation plan because if you cannot persuade or convince people to come on board and join you, then you won't be effective. That is to me the most important.

How did you acquire your communication skills?

I don't know, you just learn, you just observe and learn along the way. I'm quite fortunate to have worked for a core of good bosses over the years and saw how they did it. But you cannot just copy because if you are not that kind of personality, you can never try to be somebody else. You must understand what is your personality and be authentic, then you have to find your own way to communicate your points across.

But in order to communicate well, I think the key is to be very clear what you want to do and what is your purpose. Because I think if you're not very clear, then it is very difficult for you to be able to convince and persuade people.

First and foremost, you yourself must be convinced that this is the right thing to do. For example, with the ICA transformation plan, if I am not sure or convinced, or if I think this is just another one of those PowerPoint slides we show people – it's not going to work. I don't think you'll be able then to persuade and convince people that this is something that you must do together.

You must have feedback systems in place?

Yes, I would say to some extent we have buy in, because if not, we would not be halfway through our transformation plan, in terms of the NCC [New

Clearance Concept] and SCNG [Services Centre Next Generation] and so forth.

And which is why when I communicate, when I try to persuade them, I just zero it down to two, three key points which I think are important, so that people can remember and understand why we're doing this.

Services Centre Next Generation (SCNG)

At the services centre, ICA envisions '3N' for customers:

"No Fuss; No Visit; No Waiting".

The idea is to make our services easy to use (no fuss), digital (no visit) and if they have to visit us, no need to wait long.

We review processes and leverage technology to achieve this SCNG vision. Through these initiatives, customers can increasingly transact on-the-go, instead of having to transact face to face, over the counter.

What were the two or three key points you shared?

First point, I showed them our long term manpower challenges, the numbers – I won't go into the details.

Second point, I showed them the demands on ICA in the next 5 to 10 years, the pipeline of mega-infrastructure.

Third, I related this back to the challenges they face. Actually, most of them know what are the ground challenges when they run Woodlands Checkpoint, Tuas, airport, they know where are the constraints. They know they don't have manpower to open all the immigration counters. And they know even in today's context, with the current manpower and the current demand, they are already struggling.

All I did was to show them in 5 to 10 years' time, this is the kind of manpower that we have, this is the labour market, how it will look like in 5 to 10 years' time, and this is the demand on us. It's quite clear to me if we don't do anything now, if we

continue to do the same thing we're doing, in 5 to 10 years' time, we will have a huge problem.

I think the message sank in. Then the next challenge is how do we organize everybody, to embark on this multi-year transformation phase.

LEADERSHIP IS ABOUT BRINGING PEOPLE TOGETHER TO GET THE JOB DONE

How would you describe your own leadership style?

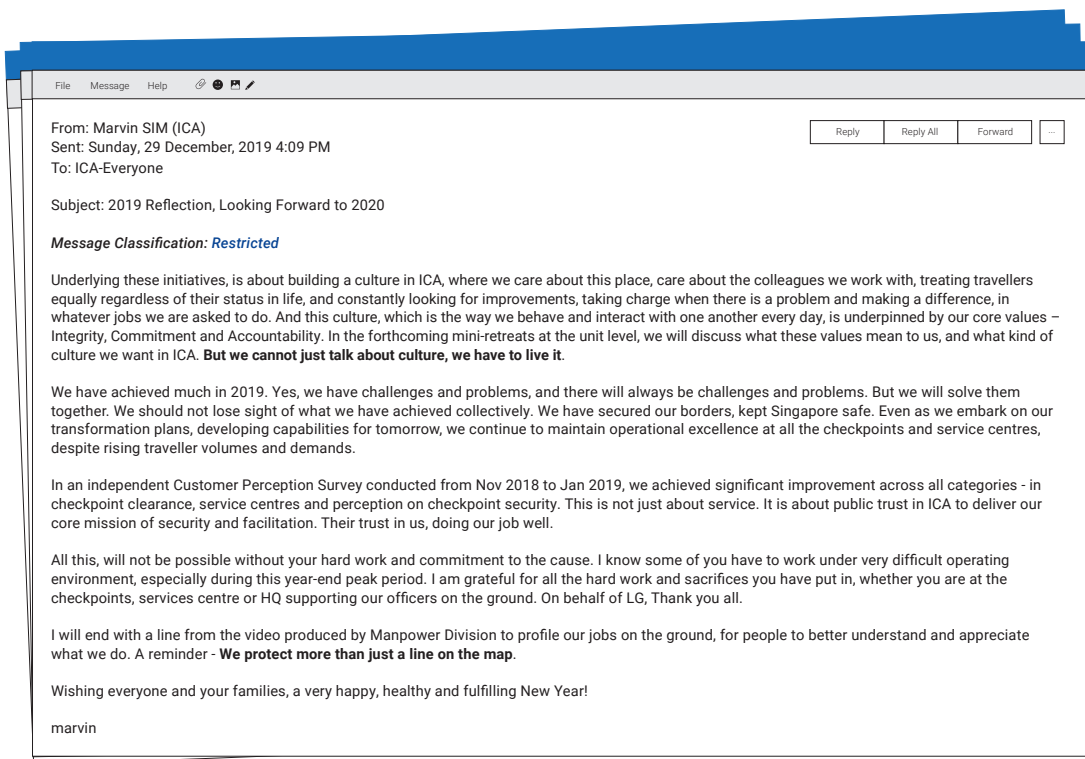
To me, leadership at its core is really about bringing people together to get the job done. Whether you're Commissioner or the deputy, or the team leader on the ground, that doesn't change it. Maybe what changes is the complexity of the task. Of course, the higher you go, the team gets larger, maybe your mission gets a bit more complex, but it's your job to have the clarity to communicate to people. So regardless which level of the organisation you're in, leadership is always about bringing people together to get the job done.

What was the moment of epiphany for you when you realised this is what it's all about?

Early in your career when you are young, you think leadership is leadership by example. I still remember when I first joined CNB, this very experienced rank and file – we used to call them detectives – told me that as a fresh graduate who joined as a senior officer, the first thing I need to do to command respect is leadership by example. Whatever the men do, you must do double. I still remember this conversation quite clearly.

So over the years, as you get wiser, as you lead more teams, you lead more different people, you realise that your context can change, the kind of people you lead have different motivations, you have to adapt. How you lead in MTI will be very different from how you lead in JOG and how you lead in CNB.

So the context can change, but the essence of it doesn't. It still requires you to bring people together to get the job done. So along the way, I realised that that's what leadership is all about. To me, leadership depends a lot on the context, the people you're leading, you must be able to understand what motivates them, what their worldview is like, what



their abilities are like, then you try to organise them in the best way possible, given the constraints, to get the job done. And along the way, you try to persuade and convince them why they need to do so.

So you need some behavioural science skills.

Yes, but after a while, after you've done different postings, you've led different teams, you roughly know that these are some of the skills, regardless of what you do and where you go, these are the things you need to do, to have the clarity of mind of what is the purpose of your job and your organisation and to be able to communicate these quite plainly to people.

So I think a key part of leadership development in the public service is also about mapping out the posting and job exposures.

This is why even today under the Public Service Leadership Programme, those who have been identified have to go through a staff posting in MHA, which I think is absolutely necessary because without that, I don't think you would get the kind of exposure. Even for myself, if I had not gone through the MTI stint, if I had not gone

through the JOG stint, I'd be quite different today in my outlook, the way I think about issues.

Joint Ops Group – that sounds like a stepping stone to HOD positions.

I don't think so. I was never told that after I do this posting, I would become a HOD. I don't think there's ever such an assurance at all. But by virtue of the portfolio in JOG, the incumbent gets exposed to operations across the whole of the Home Team. So you get a very good sense of what each of the Home Team departments are doing, you have a very good sense of the overall ministry – what are the political office holders', what are the PSEs' concerns, how they think of operational issues, and then how you have to coordinate and bring all the Home Team departments together.

When the possibility was offered to you, when you were told you were going to be Commissioner ICA, how did you prepare yourself to be an HOD? Or did they help prepare you?

Nobody prepares you for this job. It helped that in my JOG portfolio, I had some understanding of some of the longer-term challenges confronting

ICA. So when I came over, that was the first thing I did – to articulate quite clearly to everybody why there is a need for us to transform.

Some of the work had already been started by Clarence [Yeo, former Commissioner ICA]. I just needed to give a larger impetus – to organise everyone properly, put down specific timelines so that we can implement all these things.

One of the things I do, when I go to a place, is always to understand what is the mission and the purpose of the organisation, what are some of the few key challenges confronting the organisation over the next 5 to 10 years and start doing something about it.

So what is the purpose of ICA? What do you tell your staff? I know the public rhetoric, but what do you tell your staff what their purpose is?

Majority of our frontline officers are doing immigration clearance. We have to constantly remind them that at the end of the day, we are protecting more than just a line on the map. This is about securing our borders. Only when our borders are secure, Singapore gets to connect to the rest of the world, create jobs, keep supply chains moving – all these things surfaced during COVID, when the border was closed and when we were disconnected, you can see what's the impact like.

I always tell them that for a border agency, we constantly have to manage the dual mission of security and facilitation. Everything we do, from backend, approval of visas, down to the frontline border operations and every single day at all the checkpoints, up to my level, down to the last man – essentially for the Commissioner right down to the last frontline officer – our preoccupation is always about finding the right balance between security and facilitation. Maybe the complexity is different, the level of consideration is different, but the trade-off and balance is always the same, whether you facilitate, or you impose security controls.

And I always explain to some of my colleagues that in an ideal world, if we only emphasise security, then it's very easy – just close the borders. You don't need a border agency.

Sometimes the ICA officers have this impression that we are over-compromising security for facilitation. But I have to remind them our job is always about the balance and trade-off between security and facilitation. Yes, we are first and foremost a border security agency, but if security is our one and only mission, then the easiest thing to do is to just close the borders.

But that's not how it works in the real world and globalised world, Singapore needs a well-functioning border agency because we need security, and at the same time, facilitation. Our job is to do both equally well at the same time, all the time.

DURING COVID, WE WERE MONITORING 40,000 PEOPLE IN QUARANTINE AND THERE WERE CHANGES EVERY OTHER WEEK

Was this balancing act most severely tested during the COVID pandemic?

It was. For COVID, the security here is human security, in terms of making sure that the virus doesn't get imported to Singapore, especially during the early days when we didn't know what we're dealing with. And that is where the pressure and the challenge is. Every time there's a case leak, they will look to the border and find out how the case was let in through the borders.

The definition of borders got pushed inwards because you were policing people in their own homes. It's like you were creating borders around people's homes.

SHN [Stay Home Notice] was probably the largest surveillance operation that any agency has done in Singapore. At its peak, we were monitoring at one time 40,000 people on the SHN list, which means we were technically conducting surveillance on 40,000 people. That was probably the largest surveillance operation that any agency has conducted.

Of course it's not your traditional understanding of covert surveillance; this is overt, but my point is you have to watch 40,000 people, to make sure they don't leave their house. And so it was tough. And there were bound – from time to time, some leakages, but it was a challenging operation

and there were also naturally some of my ICA colleagues thinking, why are we taking on this role because like you said, it's not a border function.

We took this on because at that point in time – I still remember during one HCEG [Homefront Crisis Emergency Group] and ministerial task force meeting, we looked around our table –actually if you ask me, no one single agency was best placed to take on this task. Maybe if you argue a bit, it could be MOH [Ministry of Health]. But back then MOH was really so stretched that they were barely coping with, dealing with the crisis. The last thing they could do was to take on this surveillance of travellers. We looked around, and ICA seemed to be the most logical agency because we did the immigration clearance, we knew who they were, we had their particulars. It was quite, to some extent, natural that if you didn't have a better placed agency to take on the task, then we would take it on. Even though we were, up until now, as far as I know, we were the only border agency that did the surveillance of travellers in quarantine. None, no country, no border agency in the world was doing this. This function in other countries was taken on by health authorities. But in Singapore, I think we decided that ICA was best placed to deal with the SHN function.

What has this taught you about leadership, about innovation, management of risks, management of expectations?

First thing first, on leadership, once you have committed and believe that this is the right thing to do, then I need to come back and convince my ICA colleagues why we have to do this. It wasn't easy; because rightfully, from their perspective, they wondered why ICA should be taking on this role because this is not a border function. And I can understand why they felt that way. If I were in their position I would feel that way too. But then it was my job to convince them why we had to take it on.

Did you have big townhalls to talk to your people, over Zoom, or –

For COVID, no. I did this most of the time via email. And I explained to them that we were not the only one who were doing work beyond our mission. I gave a

lot of examples. Every time there were agencies who took on COVID-related tasks that were not related to their mission, I shared with my colleagues so that they understood they were not the only ones doing it. I think it's quite helpful that MTI, STB, EDB – many of the agencies, especially MTI took on many functions that had nothing to do with trade or industry. I also explained to my colleagues that if every agency goes to the HCEG table with the lowest denominator, many things will not be done, would not have gotten done during COVID because many of the things we did in COVID did not fall neatly into anybody's mission.

If every agency were to go to the table with the lowest denominator, I think as a country, we'll be worse off. Sometimes, you just have to find the best fit agency to take on the task and you just take it on and then you move on because things were so fluid in COVID that you've got no time to come back, hold a townhall to decide whether or not we should be doing this. Once decided, the next immediate task is to organise them to get the job done.

When you sent the emails out, did you get feedback from your staff, colleagues, did they write back?

Yeah. I also spoke to some of them, some of them fed back to me that they understood why. Of course, it's extra work, it's human nature to feedback and complain. But I think at the same time, they also understood this had to be done.

Did you do morale sensing?

Yes. As part of the COVID measures, we did. In fact, even now we do pulse surveys every six months. For COVID, I think we did it much more regularly – morale sensing every three months or so.

When we took on SHN, it would be the particular team doing the SHN that was feeling the heat and pressure, so we have to try – it's not easy, you may not be able to do it – to make sure we resource them properly to do the job.

And I think during COVID, what was equally important was to give people the assurance that they would not be taken to task when mistakes were made. I say this because what was quite challenging to us, especially at ICA, was how almost every other week,

there were changes to border policies. When there were changes, we were usually given 48 hours to implement the changes. And when there were changes, we needed to make changes to our system, we needed to communicate because all these border policies would have an impact on who we allowed into Singapore, and when we allowed them in, what do we do with them on arrival? At one point, it was 7 days' SHN, 14 days' SHN, SHN at home, SHN at hotel. I think now these are distant memories. But back then, those were operational challenges we were dealing with because almost every other week or month, there would be changes to the border policy. Now this country is under this category, tomorrow it's under another category – all these convoluted policies made it very tough for our frontline officers because pre-COVID, every day, across all the checkpoints, we cleared about 5-600,000 travellers. In order for us to clear this huge number, we require a lot of certainty and consistency in our processes. Once you start building in a variety, complexity in the process, there's no way it can scale.

And our frontline officers are not used to border policies changing every other day because pre-COVID for the longest time, from day one they joined ICA, immigration clearance is meant to be consistent and clear, so that they can clear at scale, huge numbers every day.

So these were the other challenges we were dealing with and there were bound to be some mistakes being made from time to time. I went down to the airport to assure all the officers that nobody would be taken to task for mis-clearance. In ICA's context, mis-clearance means you clear a traveller wrongly, say some Singaporeans are supposed to fall under Category A but you clear them under Category B. So I gave everyone the assurance that nobody would be taken to task for mis-clearance.

Someone's bound to complain. The public will complain.

So be it. I mean, during COVID, because at the speed at which things were moving, there were bound to be mistakes made. And the way we design the policies and processes, you will not be able to cover 100%. This is where your risk management appetite is going to come in. If you

want to move this fast with frequent changes, we try our best to do it well, to do it 100% all the time, but it's not always possible.

So we have to design the work processes to try our best to cover 90+ percent. If we feel quite confident, then we implement it. I cannot design a system or process that covers 100%. It would be too complex for our officers to be able to operationalise this on the ground.

These are some of the decisions that you as a leader have to make from time to time and then you just execute it.

OUR OFFICERS ARE MORE RESILIENT THAN WE GIVE THEM CREDIT FOR

What did the experience tell you, teach you about yourself?

If you ask me professionally, these two years were the most challenging. Not just that it was a crisis, but it was a prolonged and complex crisis; you don't know when it's going to end. That was the most challenging.

Many other crises, within 24 hours, 48 hours – you know it will end, you can get it over and done with. But COVID was one that from early 2020 till this year, before the borders reopened – for two and a half years – you really didn't know when the crisis would end and it kept changing.

So what did it tell you about yourself and your organisation?

For ICA, it told me that as an organisation, our officers are more resilient than we give them credit for.

What you want to do is make sure you organise them properly, that they try their best. It is not easy to communicate clearly some of the requirements and then look after them. These are the two or three things you need to do well during a crisis.

And I can't emphasise enough how important is the communication especially during a crisis. We communicate a lot to our people, give them regular updates, let them know what is happening, even though we do not know when the end will be in sight.

We try to be as transparent as we can reasonably tell them, so that everybody knows, down the line, what is happening.

So communication is really about communicating trust, telling your people, trust me, I've got your back, I know what I'm doing.

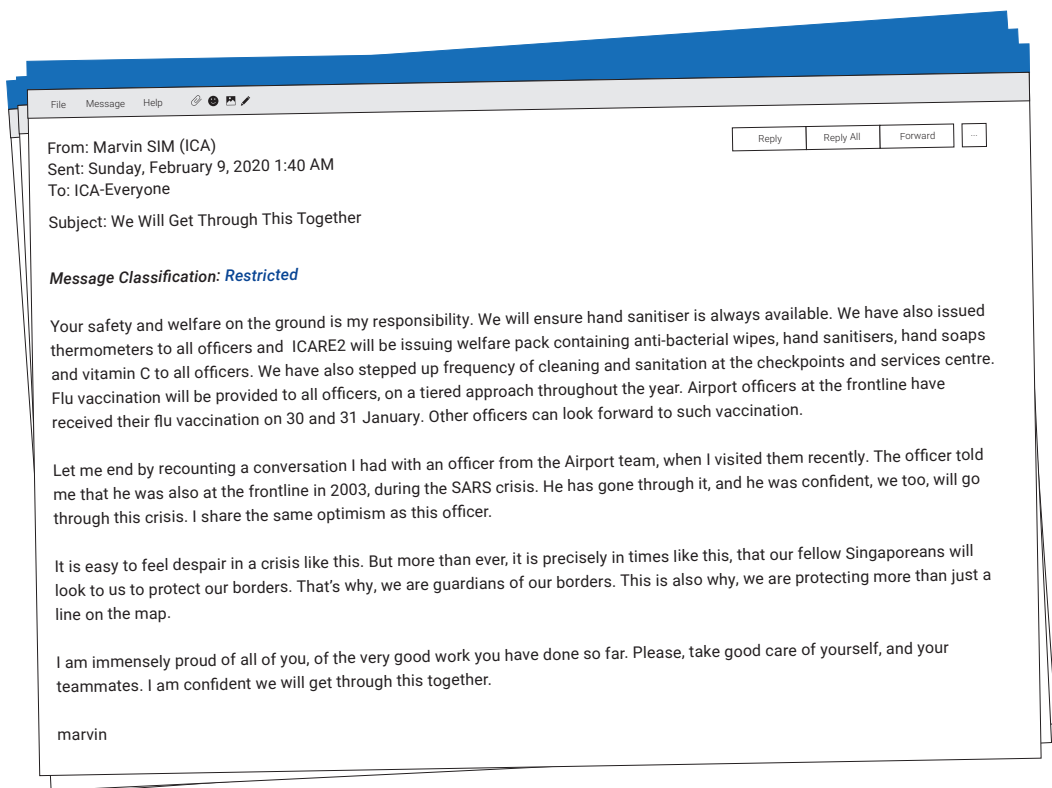
Yes. It's difficult you know, because in order to communicate these things well, you need to have built up a reservoir of trust during peacetime.

So pre-COVID, I used to go down to the checkpoints and try to meet all of the officers and speak to them in a large townhall setting, before and after their shifts. I try to reach each and every one of them. I guess those sessions helped to build some trust between us, between me and them.

And during COVID, when I couldn't meet with them, I used emails. I email everyone in ICA, so I can communicate to them directly some of my thinking, and also to update them on what is happening, what are some of the challenges that as an organisation we are facing, but at the same time, give them the confidence that we will be able to deal with COVID collectively. To me, that's important.

And pre-COVID, usually what I did for the dialogues was, after I took some of the feedback, I would try to make sure that if there were things that we could do, we would follow up and do, and then we would close the loop to tell them that it had been done. For those things that we could not do, I would also be quite frank with them and explain to them why it could not be done.

Again, to me that is the key to building trust. I think that our officers, ground officers are not unreasonable. What they want to know is you do listen, and those things that from their perspective they believe can be done, they expect them to be done. And which I agree with. Things like renovating a toilet, putting in a better canteen – these are things that we can do. Hygiene factors which are within our means to do, we should do it. If there are certain things which are beyond our control, or things that are more challenging, involving different trade-offs, I'm quite prepared to explain to them why it cannot be done, share with them from my perspective what are some of the challenges to this policy and the trade-off, why it's not as simple as it may seem. And usually, my own sensing is, people understand and accept but they just need to know what is happening, and need to know why it cannot be done.



I think these are important to do – don't brush the problem aside or sweep it under the carpet and think that everything is fine.

Is that what you think worked especially well in maintaining trust and morale.

And trust between us, between me and them. To me, that's important.

IF YOU WANT TO CROSS THE LAND CHECKPOINTS AT PEAK HOURS, YOU HAVE TO EXPECT DELAYS

More recently, there have been a fair bit of public complaints about long waits for passports, long lines at the checkpoints.

The passport waiting times and the so-called traffic jams at the land checkpoints are inter-related.

The key pressure point for us is the surge, the demands on us that we cannot shape. Of course on hindsight, the passport issue – could we have done better in terms of communication? Yes, perhaps we could have gone out earlier to urge members of public who have passports expiring to come forward earlier to renew their passports. But the issue also is that we didn't know when the border would be reopened. And even if we did, we could not go out and say so. Because we can't move ahead of the MTF [Multi-Ministry Task Force to manage COVID] to say that the border will be opening.

So on hindsight, could we have been better about it? I've been thinking about it. Perhaps we could have gone out with some more generic comms much earlier than 1st April to tell people to consider renewing their passports. But at the core of it, it's an issue of demand and supply. It's a situation whereby we have two years' worth of passports that were expired and that were not renewed. And now they are all coming forward to renew at the same time. And it's the same problem that agencies around the world face.

And so it's an issue of marshalling the resources, organising them to meet the surge in demand, so

you just have to bear with the heat in the short term. It's a problem that can be solved.

When I renewed my passport beginning 2021, I was told to collect it in two days, and I was in and out in minutes.

It's all an issue of demand and supply. So when there's a surge in demand, what do you do? You just organise your resources to meet the surge. That's the best you can do. I don't think there was any policy missteps or anything like that.

For Woodlands Checkpoint, it's a much more difficult problem, to some extent a wicked problem because for land crossings, there's a huge latent demand. I'm not trying to find excuses, but I think no matter how efficient you are – you imagine with today's exchange rate, if the checkpoint is clear and you can travel from Woodlands to JB in a matter of 10 minutes, many Singaporeans will be going over there.

So today we are seeing for the land checkpoints, a volume of about three-quarters of pre-COVID, but during peak hours it's almost back to pre-COVID levels.

Because Malaysians are going home?

No. It's more Singaporeans travelling over, either for holidays, to buy things because it's a function of the exchange rate. So in a steady state, there will be jams. The question is at what level is it tolerable, or beyond what people can tolerate.

And this is a constant balance that we always have to make. I have X number of manpower, I have to try my best to organise them optimally to be able to clear both the peak arrival and departure timing.

But you can't search every vehicle.

Yes, but at arrivals we do 100% screening post-9/11. We do 100% checks.

Woodlands Checkpoint was designed and built pre-9/11. But post-9/11, we are doing 100% arrival checks. Departure – we don't do 100% but arrival we do 100% checks. So all these have added up.

I guess you want it to be public knowledge that you do 100% checks for arrivals.

Yes, which is why for the land checkpoints, public comms plays an important part to manage public expectations that if you want to travel during the peak travel period, and we tell them when is the peak travel period and they want to travel, then they must accept and plan in advance for the jams.

But Singaporeans don't listen and then they complain. Lee Kuan Yew said we were a nation of complainers.

Yes. But that is the nature of the Woodlands Checkpoint problem and the passport wait. It's really an issue of matching demand and supply, how to organise the resources to manage the demand, and if you can't, what are the levers to try to shape the demands.

There is talk of a borderless world, and we know the Singapore passport is the second most powerful in the world after only Japan. Obviously, as you said, we still want to control who and what comes into Singapore. What does the future of border security look like?

This is related to our transformation plan. There are different degrees of borderless, right?

At one extreme, if you don't have to apply for a visa to go to a country, it's considered borderless. Then on arrival, you can use automated lanes.

Pre-COVID, we were clearing maybe slightly over one-third of our travellers on arrival with automated lanes. Under our transformation plan, the new clearance concept, we intend by 2024 to be able to clear more than 95% of arrival travellers with automated lanes.

So from one-third, to over 90%. Every 10 arrivals, more than 9 will be able to use the automated lanes. It will be a fundamental change.

Including foreigners?

Yes, everybody. So pre-COVID, out of every 10 arriving travellers, maybe only 3 used automated lanes, and the majority of them were residents.

I used the e-gates at Heathrow recently because they allow Singapore passport holders, and in less than a minute, I was done.

Heathrow only allows some countries very selectively to use e-gates, so I guess Singapore is a safe profile and they allow Singaporeans to use them.

For us, we're going to move from one-third to close to 95% on arrival via automated clearance and behind this is what I said earlier about the trade-off and finding the balance between security and facilitation and having a clear understanding of what kind of risks you are accepting when you do this, supported by our next generation of automated lanes plus the backend integrated targeting centre. Although current technology doesn't allow it yet, I foresee people may eventually be able to clear on the move without being stopped at the immigration gantry gates.

Our NCC, our new clearance concept, when it's implemented by 2024, 2025, all residents will be able to clear immigration without their passports, just based on your biometrics. So you don't need to produce your passport upon departure or arrival if you're residents. If you're a foreigner, social visitor, you can clear automated lanes with your passport.

The next step is for people to be able to clear on the move without a gantry, but today, we don't yet have a solution to stop people whom we want to stop without a gantry.

It's always about the 1%, so for example, pre-COVID – you know what NTL stands for?

Not to land.

Yes. That means on arrival, we don't allow you entry. Pre-COVID, we were denying entry to about 0.07% of travellers. That means out of every 10,000, 7 travellers were denied entry.

So you're trying to design a system, an immigration clearance system, to manage the exceptions – the 0.07%. The challenge is designing a system that does not inconvenience the 99.03% travellers who generally you will not stop and will allow entry.

Some countries design it the other way round, they design the whole system just to capture the exceptions. Because security is so important, if you don't have a way to do profiling and security to seek out those seven people, you then have to design a system to stop everybody.

For us, to move the huge volume of people and keeping Singapore connected, we need to find the right balance.

But if one of the seven is a terrorist, that'll be a real nightmare scenario.

You usually don't know who are the terrorists. But in future, when people come through, we will be collecting biometrics. The challenge is backend, we'll have to work with the relevant agencies to profile potential terrorists.

We can collect biometrics. After you collect, what do you do? How do you work out who are those that you want to have a second look or second interview? Because that's how the whole new clearance concept works – that everybody on arrival can use the automated lanes and then at the backend, how do you sieve out those that you want to have a secondary interview with, so that you don't inconvenience the rest. That's essentially the thinking behind the new clearance concept, whereas today, with the manual counters, you subject everyone to the interview. And even the interview, if you ask me, is a cursory one because when the officer is pressured for time, and there's a long queue, there's a limit to how much they can do.

In terms of wicked problems, you've talked about Woodlands Checkpoint. What are the other wicked problems?

I don't know whether you call them wicked problems, but it's always a challenge for us when we reject applications for long term immigration facilities and cannot tell them why they are rejected. Because if you don't communicate, it undermines trust in the system because people don't know why they are rejected. And then we end up having to deal with more appeals. But at the same time if we disclose the reasons, then it'll undermine our whole policy regime. And this



is not a system where you meet a few criteria, then you are confirmed. It also depends on other factors as well.

The main wicked problem we have to constantly grapple with is the Woodlands Checkpoint issue. Even if, let's say, MOF [Ministry of Finance] gives me another 500 officers tomorrow to open more counters, I believe quite strongly that even if we can clear travellers within 10 minutes, within the week, it'll be jammed again because people will react to the fact that the causeway is now clear, I can travel more often. So this is one of those wicked problems that I think you will never be able to completely solve. The challenge is finding a right equilibrium that people are prepared to accept, that this is roughly the kind of jam you can expect.

This is the key difference between airport and land checkpoints. Airport – the capacity is constrained by the flights, you know how many flights are arriving today, you know what time they're arriving, so you can organise your resources.

But land checkpoint – you're basically exposed to the whims and fancies of travellers who want to travel. This is why it is so difficult to manage the land checkpoint operations.

So what keeps you up at night? And don't tell me you sleep very well.

Not that I sleep very well, but I'm always concerned that the more we automate, the more the resiliency

of our systems become critical. When the system breaks down, the whole checkpoint operation is paralysed because every time we implement systems, we also have to give up manpower. You cannot keep on asking for money to put in more automated lanes and then retain the manpower. But up to a certain point, you have to put in maybe some redundancy, so that when the system breaks down, you still have enough manpower to deal with the problems.

Second, the longer-term challenge is manpower. I believe in the next 5 to 10 years, manpower will be a huge, huge challenge with all the new demands on us. For RTS 2026 [the Johor Baru-Singapore Rapid Transit System expected to be ready by 2026], we are supposed to clear 10,000 passengers every hour. Beyond RTS, there's 2028 Tuas Megaport and the re-development of Woodlands Checkpoint. And then you have T5 in 2035 – T5 is going to be 60%, two-thirds of the total capacity of Changi today, T1 to T4. So when you put all these mega-infrastructure projects together, where are we going to find the manpower to handle them?

Why don't you hire older people?

We tried. In fact, today, ICA's retirement age is 63 and we re-employ officers until they are around 65, 66 years.

At Ben Gurion Airport in Israel, for some of the screening processes, they use undergraduate students.

They do. In fact, all their airport screening processes are outsourced. In Singapore, we use AETOS and Certis, who can employ part-timers. But there's a limit to how much more they can do. We cannot use them for immigration clearance.

So these are some of the challenges we will face in the next 5 to 10 years.

It's a nationwide problem.

It is, it is.

What are the hard choices you have had to make?

When I reflect back, almost all the time, the tough choices I have to make have got to do with people. Whether it is taking disciplinary action against people, or moving people because they're not performing – these are all tough choices. Or making changes that affect people's livelihood.

The so-called tough choices are not so much about policy choices. To me policy choices, operational choices, crises, we will find a way to handle. The tough choices inevitably all involve affecting people's lives.

But when you have a decision to make, it has to be made.

Do they keep you up at night?

No, but sometimes you spend a lot of time pondering and thinking, is there a better option?

PEOPLE DON'T WAKE UP IN THE MORNING THINKING THEY'RE GOING TO SCREW UP AT WORK

When you look at the future of ICA in terms of the people, are you constantly on the lookout for future leaders? And if you are, what are the qualities you look out for?

We always try our best to groom and develop the officers we have. As an organisation, we can offer the opportunities, but then it's up to the individual officers whether they want to take it up. Increasingly, important traits which officers should have, which I find important, are to be able to carry people with you when you need to implement difficult tasks, and to have the ability to adapt and adjust.

To me, these are the three key important qualities that any future leader must have. In today's environment, if you cannot bring people along with you to do difficult things, then it's very difficult to operate. And then when you bring people with you, you must constantly be able to adapt, adjust and make changes quickly.

You also have a leadership framework.

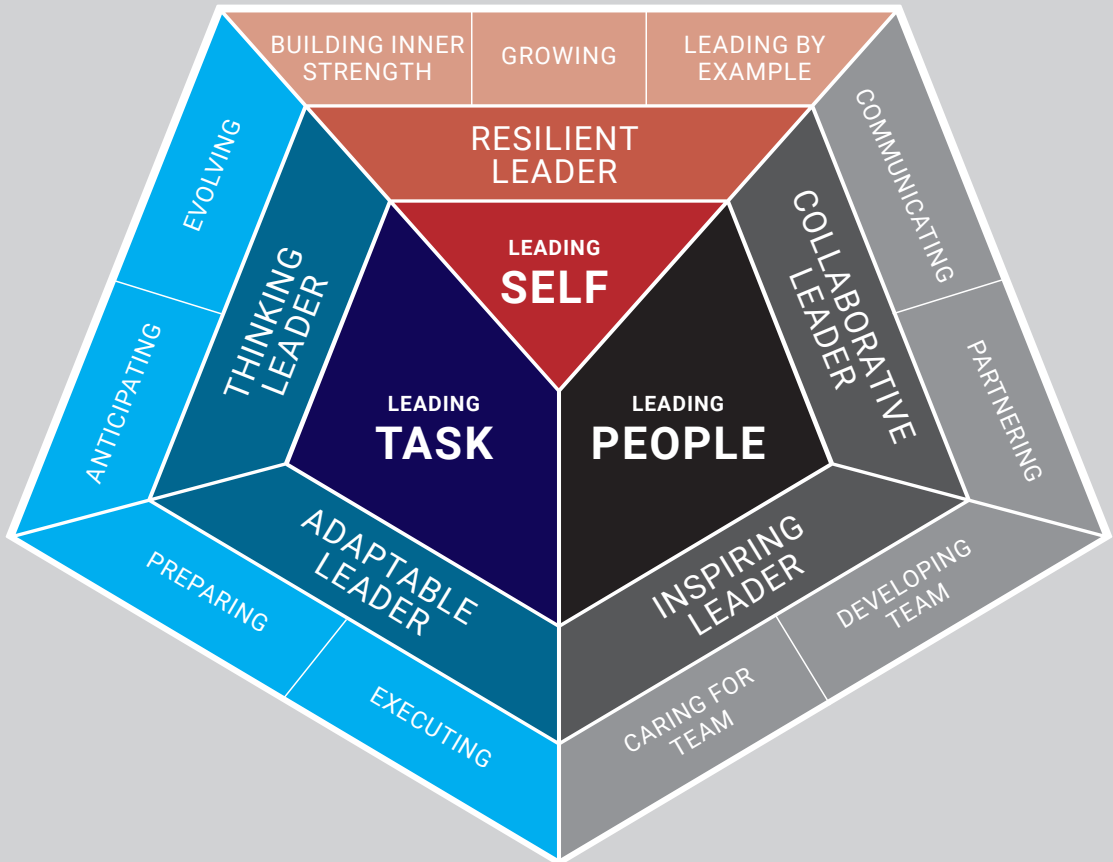
Yes, I worked with our psychology branch to put it in place based on these few qualities. I can't emphasise enough how important the ability to adapt and adjust is because things change quite quickly nowadays.

Was this a quality that you found especially relevant during COVID?

It was during COVID, but also post-COVID, as we re-open our borders. The ability to read, to understand what is changing, understand the challenges and then adapt quickly to this new

The introduction of the **ICA Leadership Competency Framework** in early 2019 helped guide the identification of competencies required for leadership development in ICA.

The framework has three focal areas – Leading Self, Leading Task, Leading People – that covers the development of 11 competencies to shape an ICA leader.



challenge, even though you may have a plan you put in place.

I also told my colleagues, even with a transformation plan which we will execute multi-year, we must be prepared to constantly adapt and adjust this plan when things change. We cannot just say we have a plan we worked out five years ago, come what may, we die die just execute this plan. We must be flexible and adaptable enough to change and adjust when we see things that are moving and not according to what we initially planned for. To me, that's important in this environment, which sometimes we are not very good at doing.

What is your personal mantra?

It's nothing high sounding. It's really that once you have decided and committed to doing something, just do to the best of your ability. This is something I constantly share with my colleagues.

The other thing I feel quite strongly about which I have shared with my colleagues, is that I always believe people don't wake up in the morning thinking that I'm going to screw up today, that you're going to go to work and make a mistake. I want to believe that most people genuinely want to go to work and do a good job. So when they make a mistake, it's sometimes because the way the policy, the system, the process is designed doesn't help them in doing their work.

I think as leaders we must always try to create a place whereby people want to wake up in the morning and look forward to going to work. Usually there are three things why people will want to go to work – the bosses that you have, the colleagues that you have, and the kind of work that you do. And these are three things everybody in the organisation can help to shape and make a difference because we are all bosses to somebody, we are all also colleagues to somebody and we all have a say in how we want to shape the work that we do. So if everybody can just contribute and do our part, generally as a whole, the place will be a much more better place to work in. This is something I believe quite strongly in and I constantly remind my colleagues

at the LG [Leadership Group] and LG-plus that we all have a role to play in this.

Has there ever been a day when you've woken up and thought, shoot, I really don't want to go to work today?

Of course, there will be. Notwithstanding what I just said, everybody has such days, right? You look at the schedule and don't think it's something you fancy yourself doing. But no choice. You can like your job but it doesn't mean you like 100% of everything, 100% of every aspect of your job. I always believe that there will be some aspects of your job that you don't like. But the question is, do you like more on the balance than dislike your job? If the answer is yes, then I think it's not bad. It is very difficult to find a job where you'll like every aspect about the job. I don't think such a job exists.

What parts of the job do you not like?

I don't know. Maybe the bureaucracies, clearing mundane approvals. It comes with the purview of the job. When I was in JOG, clearing draft PQs [Parliamentary Questions], vetting speeches – those were things I didn't like. But you know you've got to do them.

I always ask Home Team leaders what is more important to them – to be an effective leader or a moral leader?

Of course, if you have to choose between the two, moral is definitely more important. I mean that's your core values, what you personally stand for. If you compromise on those things, then I don't think you can be an effective leader because I always tell people, you know communication is important but you also must be authentic. If what you say is different from what you do, what you practise and people know it, then whatever you say is not going to carry any weight at all because people know that you don't mean what you say.

Who is the leader you most admire and why?

This one will be a cliché, but it has to be MM [Minister Mentor Lee Kuan Yew]. What I admire about him is



his single-mindedness and tenacity in getting things done, and more importantly, carrying the people with him, even though there were many tough choices that he had to make in the course of nation building, carrying not just his Cabinet, but Singaporeans too.

That's why I admire him the most. Not so much his intellectual abilities, but really his ability, his tenacity, single-mindedness to get things done when he's

committed and believe is the right thing to do, and to bring people along with him.

In the Home Team, I've been very, very lucky to have worked with many good bosses along the way who have given me a lot of room to do what I needed to do, the autonomy to do what I needed to do, and to only come in when I needed some guidance. I could not ask for more.

FINANCIAL CRIMES

SINGAPORE'S PRESIDENCY OF THE FINANCIAL ACTION TASK FORCE: FIGHTING FRAUD AND TRANSNATIONAL CRIME MORE EFFECTIVELY

T. Raja Kumar
President, Financial Action Task Force

ABSTRACT

Singapore assumed the Presidency of the Financial Action Task Force (FATF) in July 2022, following the FATF Plenary's decision to appoint him to lead the global money laundering and terrorism financing watchdog in March 2022. Soon after assuming office, Raja Kumar, the first Singaporean to head the FATF, delivered a lecture at the National University of Singapore Law School, where he laid out Singapore's FATF Presidency priorities. In this essay adapted from the lecture, he also addresses the contemporary challenges relating to financial crime and money laundering and the state of the global landscape, and the need for a "Whole-of-Society" approach to tackle the scourge of money laundering.

CONTEMPORARY CHALLENGES

Legal, banking and finance professionals have a crucial role to play in global efforts to combat financial crime, including money laundering, terrorism financing and proliferation financing. The strength and success of anti-money laundering and combatting the financing of terrorism (AML/CFT) regimes depend on both the public and private sectors working closely together to protect national reputations that are on the line. The effects of a poor Financial Action Taskforce (FATF) assessment rating extend beyond specific sectors. It also impacts on investments and the national economy, as legitimate investors tend to shun riskier jurisdictions. Those with a strong and effective AML/CFT regime have a competitive advantage in the longer term. This makes lawyers, bankers and other non-designated businesses and professions (DNFBPs) invaluable partners and allies in our **collective fight** against financial crime, as we seek to contain the bad actors and

cut off the lifeblood of criminal enterprise, which is money!

Financial crime is very much a key concern globally and is tied to a wide array of criminal activities, ranging from organised crime such as drug trafficking, human trafficking and illegal wildlife trafficking to terrorism, proliferation of weapons of mass destruction financing and beyond.

The scale of financial crime is staggering. Estimates by the UN Office of Drugs and Crime¹ suggest that the amount of money laundered globally in a year is between 2 to 5% of global GDP, or \$800 billion to \$2 trillion in current US dollars. The sharp trajectory of growth of such crimes means that the situation is poised to get far worse. As a result, financial crime can be a threat to financial stability and growth.

Financial crime results in monies funnelled away from legitimate business endeavours to criminals

¹ UNODC Overview of Money Laundering, n.d.

and criminal enterprise and the development of an underground economy, where taxes are invariably not paid and there is significant tax leakage. A UN report released in 2020² estimated that up to US\$500 billion in tax revenue was lost due to financial crime and money laundering, money that could have been used for social programmes and improving the lives of people.

The sheer scale of financial crime also presents a **long-term strategic threat** to societies and governments. Armed with high returns on their criminal misdeeds, criminals are in a position to subvert officials and entire ecosystems through corruption and constitute an even larger threat.

Fraud and transnational crime are themselves not new phenomena, but they have grown more complex and more challenging to combat, particularly with the pervasive use of technology, and the exponential growth in cross-border trade in goods and services, including online.

The COVID-19 pandemic accelerated the digitalisation trend, as lock-downs and travel restrictions led to increased reliance on digital banking and e-commerce platforms, which have become ubiquitous, part and parcel of daily life – even after most restrictions have been lifted. The benefits of convenience and the time saved by consumers is undeniable. However, the unintended consequence of this shift toward digital financial tools is that it has opened new attack vectors for criminals to target and commit crimes. Criminals have also been able to move illicit funds more rapidly, more easily than ever before – taking full advantage of technology and rapid payment systems to move their ill-gotten gains across one or more jurisdictions to mask the money movement trail.

This is a gloomy picture of the current global situation, but it needs to be painted accurately as is. We must be clear-eyed about the significant challenges that we are facing to be able to effectively deal with them.

To this end, there are multiple international stakeholders who have committed to combating financial crime.

The FATF and the FATF-style regional bodies (FSRBs) are key players in this fight against financial crime. FATF was established by the Group of 7 nations in 1989 to tackle the major threat posed by drugs by targeting related money laundering. Today, FATF is recognised for being the global watchdog against money laundering, terrorism financing and proliferation financing. It sets global standards for countries to follow and it audits countries against these standards. Its teeth come from its ability to publicly identify countries that are not taking effective action against these crimes, including by placing them on its grey-list and black-list and calling on countries to apply counter-measures to mitigate the risks they pose to the global system.

At the broader political level, the UN and G20 have both agreed that combating financial crime and corruption internationally must be prioritised. FATF is working closely together with them as well as other organisations such as INTERPOL, the Egmont group of Financial Intelligence Units, the World Bank and the International Monetary Fund.

The aim is to actively raise awareness, promote information sharing and support technical assistance and capacity building efforts to ensure that national authorities have the necessary knowledge, skills and capabilities as well as frameworks to combat financial crime and related money laundering in all its forms.

Private sector partners, such as the Wolfsberg Group, are also actively involved in this space, given their gatekeeper role and financial crime risks their sectors are exposed to. So these are the challenges we face and the partners we are working with.

FATF PRESIDENCY PRIORITIES

Having set the stage and illuminated it with current reality, let me next touch on my FATF Presidency priorities.

When Singapore was preparing its candidacy for the FATF Presidency, we took a hard look at the current reality and saw significant gaps and threats which we identified as global opportunities

²Report of High-Level Panel on International Financial Accountability, Transparency and Integrity for Achieving the 2030 Agenda, September 2020

to tackle these challenges more effectively. For example, an April 2022 FATF report found that whilst countries now have the laws in place to tackle money laundering and terrorism financing, many are not effectively implementing these laws and are not showing strong outcomes.

In response to this finding, the key theme underpinning my presidency of the FATF is to enhance effectiveness within it and across the global network to make a tangible impact and significant difference

Special Focus on Asset Recovery

In the wake of the pandemic, we have seen the rise of online cyber-crime, more specifically in fraud and ransomware. The scale of this problem is staggering. Let me cite a few examples. The US Federal Bureau of Investigation (FBI) reported over US\$6 billion internet crime losses in 2021.³ The UK Action Fraud reported over £2.3 billion in losses in 2020 and 2021.⁴ Closer to home, the Hong Kong Police reported nearly 20,000 deception (fraud) cases in 2021, a significant increase of 24%. Many other jurisdictions are experiencing the same problem, including Singapore.

Singapore saw cyber-enabled fraud/scam cases increase to a whopping 51.8% of all reported crime in 2021, up from 42% the year before. Victims of the top 10 scam types in Singapore alone were defrauded of more than half a billion Singapore dollars – S\$504.4 million to be exact.

There are ominously strong signs that the problem will grow worse as criminals further exploit this space and its vulnerabilities. It is sobering to note the UNODC estimate that only 0.7% of illicit monies were recovered by law enforcement agencies globally, which is very low.

There are three main implications of this low recovery rate: the first is that criminals continue to reap, retain and enjoy profits from their criminal activities – sadly crime is paying well; the second is that this gives criminals the resources to pose an even greater threat to society as they grow in financial muscle; and the third is that more

criminals, sniffing rich rewards, are being drawn to this space.

Beyond the statistics, the reality is that these crimes have real victims. For example, as a result of falling prey to investment scams and romance scams, many have lost their entire life savings. Some of us probably know personally of someone who has fallen victim to some kind of cyber-enabled scam/fraud. Many victims are often embarrassed to admit they have fallen for a “scam” so there are probably more victims in each of our network of contacts than we know of.

Victims range widely in terms of age, education levels and socio-economic status – but the impact on them can be life-changing. Some of their stories are truly heartbreaking. Dreams have been shattered, futures have turned bleak, some victims have gone into depression, contemplated ending their lives or even taken their lives.

Our ability to act in this area to recover and return assets to these victims can mitigate their losses, impact their lives, give them hope. This is why I have made strengthening asset recovery through effective and meaningful international cooperation one of the key priorities of my FATF presidency.

We will pursue this priority through a suite of measures, including expediting existing work on asset recovery and proposing new operational initiatives.

In June 2021, the FATF identified the operational challenges pertaining to asset recovery and developed a set of recommendations to effectively meet these challenges in different types of situations and across legal systems.

We want to drive implementation of these recommendations through close cooperation between the FATF, FSRBs and the Asset Recovery Networks that have been formed, as well as with other strategic partners such as the UN and INTERPOL.

For a start, under the Singapore Presidency, the FATF has initiated with INTERPOL and convened the FATF-Interpol Roundtable Engagement, abbreviated as F.I.R.E. It is a powerful image – we

³ US Federal Bureau of Investigation Internet Crime Report 2021

⁴ UK Action Fraud 2020-21-Annual-Assessment-Fraud-Crime-Trends

want to fire up global attention to this problem, and ignite a fire across the law enforcement community targeting criminal assets. The inaugural Roundtable was held in September this year. It involved a range of invited stakeholders from law enforcement, Financial Intelligence Units (FIUs), prosecutors, regulators, policy makers, industry experts, and leading think-tanks. It focussed on how best to tackle financial crime, in particular cross-border cyber-enabled fraud/scams and ransomware, and how best to enhance timely asset freezing and seizure.

Initial discussions focussed on the high-level strategic global financial crime landscape, zooming in on priorities and actionables for law enforcement and regulators/supervisors. This included how data analytics (DA) and public-private partnerships (PPPs) can be used to enhance and support the work of law enforcement agencies and other authorities in this space.

Sadly, crime is paying well – this gives criminals the resources to pose an even greater threat to society as they grow in financial muscle, and more criminals, sniffing rich rewards, are being drawn to this space.

The key outcome we want is to promote the actual and timely recovery of proceeds of cyber-enabled crimes relating to fraud/scams and ransomware. We hope to build this initiative into a multi-year series of roundtables that will result in concrete improvements in asset seizure and recovery over the next few years, beyond just a one-time effort.

Focus on Illicit Financial Flows linked to Cyber Fraud

In a separate but related initiative, we will also be pursuing a FATF project that focuses on the illicit financial flows linked to cyber-enabled fraud/scams. This project seeks to:

- a. Better understand the challenges and analyse the money laundering techniques that are unique to these crime types;

- b. Identify appropriate tools, including cases on data analytics and industry partnerships by law enforcement and FIUs; and finally
- c. Illuminate best practices.

Increasingly, we are seeing that some of the proceeds of cyber-enabled fraud tend to be kept and moved by criminals in the form of crypto-assets, which have grown in prominence in recent years. Ransomware is another emerging crime typology where crypto-assets are used. Criminals demand ransom payments in crypto-assets to take advantage of the anonymity they offer.

The FATF will thus also be focusing on crypto-assets and crypto-asset service providers during the next two years.

To their proponents, crypto-assets and their underlying technologies have the potential to fundamentally reshape financial systems and financial products, with the promise of greater speed, lower cost, greater accessibility and privacy. Its detractors, amongst other charges, claim that crypto-assets are easily abused by criminals, including terrorist groups, organised crime groups and even rogue states, to circumvent AML/CFT controls and evade the scrutiny of national authorities.

Increasingly, we are seeing that some of the proceeds of cyber-enabled fraud tend to be kept and moved by criminals in the form of crypto-assets Criminals demand ransom payments in crypto-assets to take advantage of the anonymity they offer.

What is undeniable is that crypto-assets have grown large enough to necessitate closer attention and international cooperation to ensure that it is not abused by perpetrators of financial crime, while still allowing for legitimate growth. For instance, in 2020, industry estimates⁵ were that ransomware payments reached over US\$ 400 million globally, more than four times the level in 2019. This estimate may be low, given that many victims do not report

⁵Chainalysis Ransomware Update, May 2021

that they have been hit and just pay up the ransom demanded in crypto-assets.

In 2019, the FATF strengthened its standards to prevent the misuse of crypto-assets, also called virtual assets, for crime or terrorism. Virtual asset services providers must be properly licensed and supervised, and they must ensure that information about the beneficial owners of transactions is available – the so called “travel rule”.

Plugging the Gaps

It is important that we ensure that FATF Standards and, in turn, national legislation and supervision, keep pace with developments. This means ensuring that the FATF Recommendations are updated when necessary, and that these changes are then effectively implemented in a timely manner by all jurisdictions.

The current reality is that there are significant gaps that need to be plugged in this space. For one, most jurisdictions are still in the midst of implementing the 2019 revisions to the FATF Standards. The implementation of the “travel rule”, intended to mitigate anonymity risks, has been slow. Two months ago, the FATF published its most recent update which noted that only 11 out of 60 respondent jurisdictions globally have passed the necessary laws and started supervisory or enforcement action in line with FATF Standards. We will need to work together to advance implementation. This is to reduce the ability of criminals to exploit the differing levels of implementation across jurisdictions to continue to commit crimes and evade AML/CFT controls. After all, a chain is only as strong as its weakest link, so all jurisdictions must be committed to expeditious implementation of all FATF Standards to ensure that the global AML/CFT regime remains robust and effective.

WHOLE-OF-SOCIETY APPROACH

The challenges posed by complex emerging issues, such as crypto-assets, highlight another point, which is the importance of adopting a Whole-of-Society approach to combating financial crime to ensure that our AML/CFT measures are effective.

Governments and law enforcement alone cannot effectively deal with financial crime. It requires a robust response at the ecosystem level. Financial institutions, e-commerce platforms, payment service providers, Virtual Asset Service Providers, FIUs and regulators all have key roles to play in the prevention, detection, disruption and prosecution of such fraud.

Speed and quality of information sharing between the public and private sectors is crucial, as rapid action is often needed to intercept transfers of ill-gotten gains from frauds and scams before they are transferred overseas.

As technology becomes further entrenched in our daily lives, those involved in this space need to go beyond a current operating paradigm of only looking at AML/CFT compliance as a hurdle to cross, often looked at only after development of a product, just before going to market.

Instead, platform developers and digital financial solution providers should consider how AML/CFT compliance can be built into such products and services right upfront at the conceptual and design stages; it must not be an afterthought.

After all, it is also in the interest of developers and operators to ensure that their products and services are not susceptible to abuse by criminal elements, given the risks involved, including legal, operational and reputational risks.

Role of Designated Non-Financial Businesses and Professions

As we all know, money laundering, terrorism and proliferation financing are not problems restricted to the financial sector alone. Key non-financial businesses and professions, in FATF-speak known as Designated Non-Financial Businesses and Professions (DNFBPs), also have crucial roles to play against such crimes. These include lawyers, company service providers, real estate agents, dealers in precious metals and stones, and accountants.

This is an area that the FATF has identified as requiring stronger national implementation by jurisdictions and closer cooperation internationally.

In some of the significant money laundering / terrorism financing (ML/TF) cases and scandals that we have observed, a vigilant DNFBP, such as a lawyer or company service provider, could have provided early information of potential misfeasance or malfeasance before proceeds of crime entered or exited the jurisdiction's financial system.

Lawyers, for instance, are involved in a wide range of activities, including facilitating real estate purchases or sales, advising on and establishing legal structures and/or arrangements such as trusts, as well as handling clients' monies. Lawyers must understand their sector's ML/TF risks, implement the relevant risk mitigation measures and act as gatekeepers. Those who are less au fait are at risk of becoming conduits or enablers of money laundering.

There are past examples where hardly any due diligence was undertaken. So "Tom, Dick and Harry" remained largely "Tom, Dick and Harry", with few, if any, questions asked about their background and sources of wealth, and no screening was done against global Know Your Customer databases.

Much has since improved here in Singapore in the past seven years, thanks to the efforts of the Ministry of Law working closely with the Law Society.

The FATF has played its part too. In 2019, the FATF published a guidance for a risk-based approach for legal professionals, to help them manage their ML/TF risks when establishing or maintaining customer relationships.⁶

Overall, while major strides have been made in collaboration with industry in recent years, such as the establishment of the AML/CFT Industry Panel (ACIP) in 2017, there is still a great deal more that needs to be done to ensure that DNFBP sectors do not become the weak links in Singapore's AML/CFT regime. These sectors need to have a comprehensive understanding of their ML/TF risks and adopt necessary measures to ensure that they are not abused by criminals.

We have found that public-private partnerships (PPPs) between authorities and the private sector, including through digital transformation, can foster more practical and pragmatic solutions than those developed separately. We therefore encourage DNFBPs to participate actively in such PPP engagements.

The PPP model is a two-way engagement. Regulators and law enforcement authorities use these platforms to provide industry with updates to keep pace with developments, such as emerging threats and modes of crime. They benefit from industry perspectives and knowledge as well as industry resources. Private sector participants on their part would have a direct channel to provide their views and obtain direct feedback from regulators and law enforcement. This is necessary to ensure a high awareness of key risks as well as exploring and co-creating approaches and solutions to mitigate these risks.

The ACIP experience has already shown us how valuable such sharing can be. Building on the data analytics capabilities of both industry and authorities, MAS, CAD and its partners are now in the process of putting in place the necessary elements for the roll-out of COSMIC (or "Collaborative Sharing of ML/TF Information & Cases"). COSMIC is truly a PPP, co-developed by MAS, CAD and six of the ACIP banks (i.e. DBS, OCBC, UOB, Citibank, HSBC and Standard Chartered). It will enable financial institutions to securely share information on customers or transactions when they cross material risk thresholds.

While the initial focus of COSMIC will be on priority risk areas for Singapore relating to legal persons, trade-based money laundering and proliferation financing, the plan is to progressively expand COSMIC to include more banks and other emerging risk areas in the future. This initiative has attracted global attention, as it holds much promise, and it is crucial that we work together to deliver on the results and be more effective in fighting priority crimes collectively.

⁶ <https://www.fatf-gafi.org/media/fatf/documents/reports/Risk-Based-Approach-Legal-Professionals.pdf>

In concluding, let me say that all of us involved in the fight against financial crime have our work cut out for us. The challenges continue to grow in both scale and complexity, with emerging technology and new methods of storing and moving criminal assets adding to the litany of challenges that we face. Ensuring all the pieces are in place, including the right laws, knowledge, skills and competencies, tools as well as platforms and frameworks, is no small challenge and there are mountains that still

need to be scaled, both at the national and global levels. Despite the scale of the task before us, I believe that with a strong sense of mission and purpose, determination, perseverance and resilience, as well as leveraging partnerships between the public and private sectors, we will each rise up to the task. With our collective and shared goal, I am confident that we will ultimately prevail in this fight against financial crime and criminals.

ABOUT THE AUTHOR



T. Raja Kumar

began a two-year term as President of the Financial Action Task Force (FATF) on 1 July 2022. He has rich leadership and operational experience, having held a wide range of senior leadership roles in the Ministry of Home Affairs and in the Singapore Police Force for over 35 years. He served as the Deputy Secretary (International and Training) at the Ministry of Home Affairs and before that as Deputy Commissioner of Police (Policy), Chief Executive of the Home Team Academy and Chief Executive of the Casino Regulatory Authority now known as the Gambling Regulatory Authority. He currently serves as the Senior Advisor (International) in the Ministry of Home Affairs, advising on international policy development, partnerships, and engagement. Raja is a passionate advocate for the FATF and firmly believes in FATF's mission and ability to make a global difference. He led Singapore's delegation to the FATF from January 2015 to June 2022 and was the co-lead for Singapore's national Inter-Agency Committee on AML/CFT.

ORGANISED CRIME COMMUNICATIONS

INFILTRATING ENCRYPTED CRIMINAL COMMUNICATIONS: THE AUSTRALIAN FEDERAL POLICE'S OPERATION IRONSIDE

Nigel Ryan
Australian Federal Police

ABSTRACT

Criminal use of international encrypted communications presents a serious challenge to law enforcement. In 2018, the Australian Federal Police (AFP) conceived a gang-infiltrating operation to expose the encrypted messages of organised crime syndicates, giving a clearer understanding of how members of criminal networks work and interact. Operation Ironside tapped the technical expertise and creative thinking of three AFP members – and their US Federal Bureau of Investigation (FBI) counterparts – in using a “trojan horse” app, ANØM. A significant departure from previous criminal disruptions to dedicated encrypted communications platforms, ANØM was developed and deployed to infiltrate criminal networks. In the four years leading up to the resolution phase of Operation Ironside, the uptake of the ANØM-encrypted communications platform and the trust criminals placed in it became clear. To date, Operation Ironside has seen the arrest of 390 offenders on 2,351 charges across Australia, and the seizure of 6,655 kilogrammes of drugs and over A\$55.6 million. The results have also been global, with hundreds of international investigations and arrests through the efforts of the FBI and a number of partner law enforcement agencies. The criminality uncovered to date under Operation Ironside is, however, just a drop in the ocean.

AUSTRALIA'S DIGITAL SURVEILLANCE OF CRIMINAL NETWORKS

The Australian Federal Police's (AFP) digital surveillance program dates back over 15 years to a time when organised crime shifted its communications to encrypted devices and the “dark web”. Since then, the AFP's technical knowledge and engineering resources have been involved in disrupting some of the largest, dedicated encrypted communications platforms in the world, working hand in hand with international partners to contribute technical expertise to facilitate the lawful infiltration and takedown of “Phantom Secure” in 2018, “EncroChat” in 2020, “SkyECC” in 2021 and now “ANØM” through Operation Ironside.

The concept for the AFP's encryption-busting, gang-infiltrating Operation Ironside emerged from three like-minded and passionate AFP members –

and their US Federal Bureau of Investigation (FBI) counterparts – thinking “outside the criminal box”. Their technical expertise and creative thinking about previously anonymous criminal communication methods enabled law enforcement to use a “trojan horse” app to expose encrypted messages, giving a clearer understanding of how members of criminal networks worked and interacted.

Australia was an ideal launch pad for this new international encrypted communications platform, known as “ANØM”, due to the comparatively high use of these platforms in Australia, in part a result of broader public knowledge about the ease with which normal telephone communications can be intercepted by law enforcement.

Since 7 June 2021, more than 4,000 members from the AFP and Australian State and Territory Police have been involved in the execution of hundreds of

warrants under the operation. To date, Operation Ironside has seen the arrest of 390 offenders on 2,351 charges across the expanse of Australia. The results were also global, with hundreds of international investigations and arrests through the collaborative efforts of the FBI and a number of partner law enforcement agencies.

The resolution of Operation Ironside is a significant milestone, exposing the previously hidden communications involved in transnational serious and organised crime – including intelligence on plots to kill, mass global drug trafficking, and firearm distribution.

It was also a significant departure from earlier disruptions to dedicated encrypted communications platforms, as this involved the sustained development and deployment of a platform deliberately designed with law enforcement to infiltrate criminal networks, whereas earlier operations had involved infiltration of existing and established platforms with a strong criminal user base.

The AFP's disruption of encrypted communications has not ended with Operation Ironside. New Australian Government legislative powers introduced in September 2021 after the resolution of Operation Ironside give the AFP and Australian Criminal Intelligence Commission (ACIC) further leverage to pursue more criminals relying on technology to facilitate, obfuscate and anonymise their criminal activities.

The Surveillance Legislation Amendment (Identify and Disrupt) Act 2021 (SLAID Act) gives the AFP new warranted powers in three major areas: data disruption, network activity and account takeovers. This allows the AFP and ACIC to target, investigate and collect intelligence and evidence against criminals who use the dark web and encrypted technology, and then use those same technologies to infiltrate their networks or disrupt their criminal activities.

THE BIG ENABLER: ANØM

Encrypted communication is a significant enabler of transnational serious and organised crime. Criminals need a mechanism to communicate in secret, and criminal facilitators need a product to address the needs of their criminal clientele. The challenge for law enforcement is how to exploit

this need so that investigators can not only see the content of criminal communications but also better understand how criminal networks work and interact. In the four years leading up to the resolution phase of Operation Ironside, the uptake of the ANØM-encrypted communication platform made clear the trust criminals place in such products. It also showed that encrypted communications is an international problem requiring an international solution.

The AFP's partnership with the FBI brought together the right skills, knowledge and legal instruments to pull off this ambitious operation. The FBI facilitated a confidential human source, who had been developing a dedicated encrypted communications platform to an expectant market following the takedown of Phantom Secure. The challenges for the AFP and FBI included navigating and aligning technical, logistical and legal requirements, including resolving how to facilitate law enforcement access to the content of the communications both technically and legally, while maintaining the principles required of a platform employing and maintaining end-to-end encryption and catering to a clientele fastidious about anonymity.

Working closely with the FBI and their human source, the AFP facilitated and tested a means to enable access to content, while in parallel navigating a legal framework where such an ambitious approach to infiltrating criminal networks had never been attempted before.

The AFP's technical expertise, combined with existing provisions in Australian legislation and demand among its criminal elements for secure and trusted communications, meant that Australia was in the best position to leverage this opportunity, and to deliver and refine the capability before operations were expanded into other countries.

The ANØM Platform – what is it?

The ANØM handset is a customised phone, existing solely for the purpose of secure communications. It can't make standard phone calls or browse the internet and there is no SMS functionality. It can only be used to contact other users of the platform.

The app, with the appearance of a calculator application, was pre-loaded onto the handset prior to being distributed, and it's through this app that users

made use of the encrypted functions of the phone. The phone could be wiped by the user through the input of a duress pin as well as remotely.

Using the app, the handset user could send and receive self-expiring encrypted texts, photos and short videos. The handset also enabled encrypted short voice messages, similar to the functionality of a walkie-talkie albeit with the added security of voice distortion. In addition, photos could be cropped and pixelated prior to being sent. The handset also had a “stealth mode” to give it the appearance of an ordinary phone with the inclusion of a number of fake apps.

The devices could only be obtained through criminal contacts and distributors. To obtain a handset, individuals needed to know a reseller and buy it through a covert transaction. Devices cost between \$1,500 and \$2,500, which included a six-month subscription to the platform. Subscription renewals could be purchased for up to \$1,500 for a further six months. All this functionality along with the distribution and cost models was to give the appearance of this being another dedicated encrypted communications platform and all required a strong understanding of these platforms to successfully mimic this.

When introduced, users demonstrated their complete confidence in the system – with no one speaking in code outside of normal criminal speak. Outlaw motorcycle gangs were prominent users of the platform, including the Comancheros, Lone Wolves and Rebels.

THE OPERATION – HOW IT PLAYED OUT

Operation Ironside is the largest operation the AFP has ever run or been involved in, and it has provided Australian law enforcement with an unprecedented insight into the scale of transnational serious and organised crime and its impact on the Australian community. The AFP could not have done this alone – domestic and international partners were vital to the success of the operation.

The operation commenced in 2018 with the initial distribution of 50 phones. As the uptake in ANØM devices increased, so too did the coverage of organised crime activities in Australia and around the world. International uptake increased

substantially following the takedown of Encrochat and SkyECC. More a result of timing and having a quality appealing product than a calculated move, this opened the door for a substantial increase in distribution and usage internationally.

A number of organised criminal heavyweights – including representatives from the Australian Mafia, Asian crime syndicates and outlaw motorcycle gangs – played a critical role in the growth of ANØM, distributing the devices across Australia and internationally to other organised criminals.

Two particularly influential individuals involved in the distribution of the devices were key to the operation’s success. They acted as the equivalent of current, modern day social media influencers for the criminal fraternity, unwittingly promoting the product and contributing to its success. One was the “Mafia Man”, an Adelaide businessman with significant family links to the Calabrian Mafia, involved in international drug-trafficking on a commercial scale. The other was Hakan Ayik, who had been living in Turkey for many years evading Australian law enforcement. He is suspected of directing and organising commercial-scale drug importations into Australia and other countries.

A number of other serious criminals who are well known to Australian and foreign law enforcement also used the platform.

DISRUPTION, RESOLUTION & INSIGHTS

The expansion in usage of ANØM meant a significant growth in the resources required to monitor and support the operation. Due to a number of operational and legislative factors, the decision on the timing of the final resolution of Operation Ironside was made in conjunction with the FBI.

The AFP commenced overt action in this final resolution phase in the early hours of June 7 2021. In the days of action on 7-8 June 2021, more than 4,000 AFP, State and Territory Police were involved in executing warrants across Australia.

While a large volume of arrests came in June 2021, the AFP and state and territory law enforcement had been acting on intelligence identified through the platform since the commencement of Operation Ironside in 2018. They uncovered some significant

criminal activities including acts of violence, the full spectrum of the drug trade – including the importation, manufacture, and trafficking of drugs to the Australian community – and the proceeds of crime from drug sales. Many of these were either acted on by the AFP or its State and Territory Police colleagues – and have resulted in substantial arrests.

Before resolution, the FBI – through the Europol Operational Taskforce – coordinated communication with foreign law enforcement agencies which had also been undertaking targeted activity prior to resolution. On 31 August 2021, the Europol Operational Taskforce, which oversaw the global resolution of these operations, reported that the AFP and its partners had arrested 993 people, executed 1,041 search warrants, and seized over 42 tonnes of drugs and 220 firearms.

As of 29 January 2023, Operation Ironside has resulted in 390 offenders being charged and 2,351 charges laid. Some 6,655 kilogrammes of drugs

and over A\$55.6 million has been seized, and six clandestine labs dismantled. The activity occurred through 780 warrants executed across Australia. While arrests and seizures continue, the operational disruption outcomes are still being analysed.

The AFP has also used the data from Operation Ironside to understand criminal markets and methods, including drug supply chains, concealment and import methods. Operation Ironside gave insights into the ability of criminal syndicates to rapidly adapt to challenges, including supply chain restrictions due to the COVID-19 pandemic. It also revealed the interconnected nature and collaboration occurring across criminal groups who had previously been thought to be in direct competition and working independently of each other.

Interestingly, Operation Ironside data explained why some supply chains were more popular than others; the Australian domestic drug markets have strongly-held preferences regarding the quality of the drugs.



NEXT STEPS

The extent and scale of organised crime in Australia has been laid bare. It is resilient and adaptive, posing a real threat to the community.

But criminals are now concerned about who is watching or listening to their communications, so some have returned to drug deals of the old days – even in their swimwear at the beach having face-to-face conversations to show they do not have listening devices on them.

Serious organised crime groups have no understanding of AFP's capability or what its next move will be. As it goes to war with organised crime, the AFP will only ever be as good as its connections with international law enforcement. "All of us together – are the biggest syndicate in the world."

Given the level of trust that criminals place in dedicated encrypted communication platforms, the criminality uncovered to date under Operation Ironside is just a drop in the ocean.

ABOUT THE AUTHOR



Nigel Ryan

Assistant Commissioner with the Australian Federal Police (AFP), has 27 years of policing experience. From 2008 to 2013, he was the advisor to the Commissioner of Police for media and political issues. Between 2013 and 2015, he was responsible for the implementation and management of the Federal Government's National Anti-Gangs Squad initiative. During 2014, he was responsible for the AFP's coordination of the MH17 disaster in the Ukraine and the response from the Australian Government. Ryan was promoted to Commander in 2017 as the Manager responsible for the AFP's International Engagement and International Liaison network and performed the role of Commander Professional Standards from 2018 to 2019. Since 2002, he has been a recognised drug expert after having studied with the National Crime Squad of England and Wales at Cambridge University. This work has also resulted in an ongoing role with the National Rugby League as the AFP's drug liaison and presenter to the player register. He has also provided drug presentations to a range of high-profile Australian sporting teams.

Ryan has a Bachelor Degree in Policing Studies, a Diploma in Project Management and a Graduate Certificate in Applied Management. He attended the Defence and Strategic Studies Course at the Centre for Defence and Strategic Studies at the Australian Defence College in 2016, graduating with a Master of Arts (Strategic Studies) from Deakin University. He was promoted to the rank of Assistant Commissioner in 2019, holding the role of Chief of Staff; and since July 2020 has performed the role of Assistant Commissioner Crime Command, where he has responsibility for a broad remit including Intelligence & HUMINT, Covert & Technical capabilities, and operational strategy relating to Transnational, Serious and Organised Crime. Ryan was also the senior responsible officer in the AFP for Operation Ironside, including managing the global and domestic resolution in 2021. In June 2022, he was awarded the Australian Police Medal in recognition of his distinguished service, particularly in relation to drug enforcement, crime disruption, and international policing.

TECHNOLOGY-FACILITATED CRIMES

THE EMERGING THREAT OF SEXUAL VIOLENCE IN THE METAVERSE

Karthigan Subramaniam & Kwek Boon Siang

Home Team Psychology Division, Ministry of Home Affairs, Singapore

ABSTRACT

The COVID-19 pandemic has accelerated people's desire for more immersive ways to connect with others. With the creation of the metaverse, some companies (e.g. Google, Microsoft, Apple) have begun experimenting with immersive technologies such as Virtual Reality (VR) and Haptic (i.e. touch) technology where users can navigate metaverse platforms as personalised avatars. Immersive technologies that integrate the physical world with digital or simulated reality enable a user to naturally interact with the blended reality. Against this backdrop, this brief (i) highlights how sexual violence in the metaverse occurs, (ii) examines the psychological impacts of sexual violence in the metaverse, and (iii) discusses implications for sexuality education, and the shared responsibility of digital developers, policymakers, VR headset owners, and society.

HOW REAL IS THE METAVERSE?

In late 2021, Nina Jane Patel reported that her avatar (see Figure 1) was sexually assaulted by four male avatars on *Horizon Venues* – Meta's (Facebook) metaverse platform (Patel, 2021). Although it was her avatar that was sexually assaulted in the metaverse, Patel felt psychologically distressed from her experience and froze.

Such unsolicited digital sexual interactions persist and evolve with the technologies in which they occur (Sparrow et al., 2020; Wiederhold, 2022; Wong & Hacıyakupoglu, 2022). In recent years, the metaverse, virtual reality (VR), and haptic (i.e., touch) technology have gained popularity in part due to the COVID-19 pandemic which limited in-person social interactions (Lin, 2020; Petrock, 2021).

The metaverse refers to persistent, immersive 3D virtual spaces that users can access using avatars through virtual reality headsets (Hackl, 2021). Virtual reality and haptic technology enable users to believe that they are physically present in a virtual environment by simulating real-world sensory feedback, e.g., visuals, sounds, and touch (Suh & Prophet, 2018; Wiederhold, 2022). This



Figure 1. A screenshot of Nina Jane Patel and her avatar in *Horizon Venues*

heightens the level of immersion and presence users feel in the virtual world, further blurring the lines between the real and virtual world (Suh & Prophet, 2018).

The metaverse is a broad concept with the potential to transform various sectors of the economy, including entertainment, banking, and tourism. The training sector could boost skill development in the metaverse by using real-world scenarios and high-pressure situations (Purdy, 2022). At an individual level, users could perform various activities in the metaverse ranging from meeting friends to attending work meetings and concerts (Arora, 2022). In fact, a local couple were



Figure 2. Singapore's first metaverse wedding in *The Sandbox*

the first in the world to hold their wedding (see Figure 2) on the metaverse platform *The Sandbox* (Ng, 2022).

Haptic wearables are increasingly being integrated into the metaverse to further blur the separation between the virtual and physical world (Wang et al., 2019). They could range from gloves to vests and even full body suits (see Figure 3) and use vibrations to provide accurate physical sensations. This could result in sexual violence in the metaverse being as traumatic and distressing for victims as in the real world.



Figure 3. An illustration of a full body haptic suit

And as shown in Patel's case, the metaverse can facilitate sexual violence. In fact, the Center for Countering Digital Hate (2021) observed one incident of abuse and harassment every seven minutes in a metaverse platform known as *VRChat*. This article thus seeks to highlight the emerging threat and psychological impacts of sexual violence in the metaverse, and discuss educational, policy, and social solutions to address them.

SEXUAL VIOLENCE IN THE METAVERSE

1. Sexual Harassment and Assault

Online gaming is generally perceived as a predominantly male activity in which females are afforded a secondary status compared to males (Easpaig & Humphrey, 2016; McLean & Griffiths, 2018; Smith, 2016) and tend to be the target of sexual harassment (Gray et al., 2017). As of 2020, 41% of video gamers in the United States and approximately 40 – 45% in Asia were females (Yokoi, 2021). Despite females accounting for a sizeable proportion of the gaming population over the years, sexism and sexual harassment continue to persist within online gaming communities (Smith, 2016).

For example, a female gamer who was playing *Team Fortress 2* received numerous inappropriate sexual questions (e.g., "What are you wearing? Have you any pics? Have you got any nude pics?") from other players once she began speaking in-game (O'Halloran, 2017). Comparatively, the intrusion of one's personal space and threat or violation to one's virtual body is no longer limited to a screen in the metaverse (Cortese, 2019; Low & Subramaniam, 2022).

In a survey conducted with 609 virtual reality users, 49% of female users and 36% of male users reported having at least one previous encounter with sexual harassment in virtual reality (Outlaw, 2018). These included acts of virtual groping, being "humped" by others, and receiving "thrusting" gestures in one's face. Such findings suggest that Patel's experience in the metaverse was not an isolated incident.

2. Online Sexual Grooming of Minors

Grooming refers to the process by which a trusting relationship is formed with a young person, typically with the intent of sexual exploitation or abuse and can take place on online platforms (Media Literacy Council, 2020). While most metaverse platforms require users to be aged 13 or older, there is currently no age or identity verification in place. In other words, a 10-year-old child could declare to be a 30-year-old adult, and a 30-year-old adult could pretend to be a 10-year-old child.

Table 1.Examples of sexual violence in the metaverse

S/N	Platform	Individual	Experience
1	<i>Horizon Worlds</i>	SumOfUs researcher	Led into a private room at a virtual party where she was raped by a user who kept telling her to turn around so he could “do it from behind while users outside the window could see”
2	<i>Population One</i>	Maria DeGrazia	Abused while wearing a <u>haptic</u> vest when another player groped her avatar’s chest.
3	<i>Echo VR</i>	Sydney Smith	Encountered “lewd, sexist remarks” while another player claimed to have “recorded her [voice] to jerk off”. After the incident, Smith described having difficulty reporting the player in the game.

In such instances, individuals could potentially meet children using child-friendly avatars and gain their trust in the metaverse before engaging in private video chats or interacting offline which increases the risk of sexual exploitation (Gillespie, 2020). In their research, Allen and McIntosh (2022) have come across children in metaverse platforms (e.g., *Altspace*, *VRChat*, and *Horizon Venues*) who were as young as six interacting with adult strangers. They note that compared to non-immersive online spaces (e.g., chatrooms) where strangers mainly communicate and share content, embodiment in metaverse platforms allow strangers to physically interact through their avatars which could facilitate sexual grooming.

An Economist Impact survey in 2021 also found that 34% of respondents were asked to perform sexually explicit acts online during childhood. In addition, from 2019 to 2020, there was a 77% increase (of which 80% came from girls aged 11 to 13) in child self-generated sexual material (Internet Watch Foundation, 2021). Multiple media articles have similarly highlighted the risks of children in the metaverse. For example, a nine-year-old was using their parent’s virtual reality system in *Horizon Worlds*, which has an age limit of 18 years old (Oremus, 2022). In another case, an avatar with a deep voice was seen telling a fairy avatar with a child’s voice, “I just want to put you in my pocket and bring you home, little fairy girl. [I would] put you in my sink and give you a bubble bath” (Roper, 2022). Others have similarly reported witnessing children being forced to engage in simulated sexual acts in virtual reality, as well as a seven-year-old girl who was surrounded by men who threatened to rape her (Allen & McIntosh,

2022). In South Korea, an individual was sentenced to four years in prison for lying about his age and using a young person’s avatar to collect sexual content from minors (Park, 2022).

Exposure to Sexual Material

The metaverse also allows users to meet others through their avatars by visiting virtual rooms which have no age restriction. Some of these rooms resemble strip clubs and others have avatars simulating sexual acts. When a BBC news researcher posed as a young teen and explored *VRChat* with her virtual reality headset, some users spoke to her about “erotic roleplay”. Notably, one user told her the app had features that allowed avatars to “get naked and do unspeakable things”. She was also approached by several adult avatars and shown sex toys and condoms (Crawford & Smith, 2022). She described:

There are characters simulating sex acts on the floor in big groups, speaking to one another like children play-acting at being adult couples . . . [It is] very uncomfortable, and your options are to stay and watch, move on to another room where you might see something similar, or join in - which, on many occasions, I was instructed to do (Crawford & Smith, 2022).

A user also attempted to perform sexual acts on the researcher’s avatar while another claimed that he would “rape [her] little sister” after he had sex with [her]. Another journalist who posed as both a 22-year-old woman and a 13-year-old girl reported similar findings. Rose and Phillips (2022) reported that apart from witnessing the simulation of

sexual acts (including users who appear to be minors), the journalist was:

- Repeatedly approached and threatened by an avatar who asked her to reproduce with him and asked, “who’s going to stop me?”
- Asked by another user, “you like getting head from minors?” before simulating a sexual act.
- Told by another user that they like “little girls between the age of nine and 12”.

A concern related to the exposure to sexual material is that of sexual ageplay. It involves consenting adults who intentionally simulate child abuse by choosing child avatars to engage in child-child or child-adult sexual activities within the virtual world (Reeves, 2018). While sexual ageplay by itself may not be a crime as the participants are consenting adults, such forms of role-playing may normalise this behaviour for onlooking children and facilitate sexual grooming.

THE PSYCHOLOGICAL IMPACT OF SEXUAL VIOLENCE IN THE METAVERSE

Eliciting Real-life Sexual Victimization Responses and Psychological Trauma

Virtual sexual harassment has been an enduring component of online platforms since the earliest days of the internet (Wong, 2016). In the past, such abusive interactions were generally confined to verbal and visual sexual messages. Hence, they were often dismissed and downplayed as experiences that were not real (Franks, 2017). This has led to digital dualism – a misconception that online abuse is less real just because it happens behind a screen (Jurgenson, 2011).

The truth is that sexual violence in the metaverse could be as emotionally evocative as real-life sexual violence experiences due to its level of immersion and realism (Slater et al., 2006). According to Katherine Cross – an online harassment researcher – virtual reality spaces are designed to trick the human brain by simulating the real world as closely as possible (Pang, 2022). By doing so, virtual reality triggers the same psychological, emotional, and bodily response although a person’s physical body might not be touched (Pang, 2022). Individuals who experience sexual violence in the metaverse may exhibit similar fight or flight responses (e.g., increased heart rate) as

those who experience sexual violence in real life (Wiederhold, 2022). Beyond the psychological trauma caused by the incident itself, individuals such as Patel have received offline death and rape threats and threats against her daughters (Singh, 2022). Consequently, such traumatic experiences in the metaverse could affect individuals both psychologically and physically even when offline (Wiederhold, 2022).

When engaging with non-immersive forms of media, emotions are experienced vicariously through one’s avatar, putting physical and psychological distance between the self and avatar (Lin, 2017). However, sexual violence in the metaverse could be psychologically traumatising as users now directly experience these emotions using a first-person embodied perspective. According to Jesse Fox, an associate professor at Ohio State University, individuals who highly identify with their avatars and portray themselves in an authentic manner would feel violated when their avatars are abused, and it would feel similar to sexual violence in real life (Basu, 2021).

Past research into sexual abuse in virtual reality suggests it is linked to a greater sense of presence and enhanced negative emotional responses that could linger beyond one’s virtual experience (Lavoie et al., 2020; Pallavicini et al., 2018). The findings suggest that sexual violence experienced through virtual reality in the metaverse could elicit enhanced fear and anxiety responses, potentially causing the user significant distress and psychological harm.

Haptic technology could cause greater psychological trauma as it enables users to experience touch feedback. Compared to non-physical sexual trauma (e.g., verbal sexual harassment), sexual trauma involving physical contact has been associated with greater apprehension and avoidance towards being touched by others (Christensen, 2016). Additionally, compared to victims of non-contact sexual trauma, victims of contact sexual trauma have reported greater impairment to their daily functioning although both groups experience traumatic consequences. (Pinchevsky et al., 2019). Hence, these findings suggest that touch plays a significant role in trauma.

Factors influencing trauma responses

In general, many factors influence one's intensity and pattern of reactions to trauma (Perez & Hazell, 2011). For sexual violence in the metaverse, this includes one's extent of self-identification with the avatar and age. Firstly, personalised avatars that closely resemble one's real-world appearance significantly increase one's perceived presence in the virtual environment and body ownership (Waltemate et al., 2018). Consequently, the extent of self-identification with one's virtual avatar might result in a substantially more direct and greater experience of trauma.

Secondly, trauma has more serious effects on younger victims, and interferes with the developmental stage at the time the trauma occurs (Perez & Hazell, 2011). Thus, adolescents are a particularly vulnerable population of sexual violence in the metaverse. As adolescence is a critical period for sexual and identity development, negative sexual experiences are likely to have a particularly detrimental impact on adolescents' self-concept (Turner et al., 2010). For example, in a study by Turner and colleagues (2010), only sexual victimisation independently reduced adolescents' self-esteem when compared to other forms of victimisation (e.g. peer victimisation and non-sexual child maltreatment).

Child sexual abuse victims who were groomed online have also reported acts of self-harm, and feelings of depression, hopelessness, shame, embarrassment, and humiliation (Quayle et al., 2012). They have also cited relationship avoidance and difficulties, supporting the notion that childhood sexual trauma can interfere with one's ability to develop and maintain close, intimate relationships with others (Yuan et al., 2006). Furthermore, compared to adults, children react to and cope with trauma less effectively as they have a reduced capacity to organise, integrate, make sense of, and articulate their traumatic experiences (Perez & Hazell, 2011).

Long-Term Consequences of Virtual Sexual Trauma

Similar to offline sexual abuse, the sexual trauma experienced by individuals in the metaverse could have significant short-term and long-term consequences. These consequences include

immediate distress after the incident, such as shock, fear, and social withdrawal, as well as post-traumatic stress disorder (PTSD) symptoms like insomnia, hypervigilance, and flashbacks (Yuan et al. 2006). Among female college students, sexual victimisation is associated with greater health risk behaviours, e.g., increased substance use, and risky sexual behaviours (Turchik & Hassija, 2014) and could lead to negative beliefs concerning esteem, trust, and safety (Thompson & Kingree, 2010).

Increased Victim Blaming

Victim blaming is a common response to both offline and online sexual violence. Victim blaming involves individuals attempting to rationalise or minimise the behaviours of a perpetrator by attributing part or all of the blame to the victim (Sugiura & Smith, 2020). Often, violence is perceived to be a physical act and consequently, the real-world impact of virtual sexual violence tends to be downplayed and dismissed by many (see Figure 4, Franks, 2017). When Patel (2021) recounted her experience in a Facebook group, some of the comments included "some people just have to feel like victims no matter what" or "omg these females are getting out of control just please press the exit button smh". Such attitudes and mindsets place the onus on victims to take extra steps to secure their safety by leaving or avoiding metaverse spaces and activities.

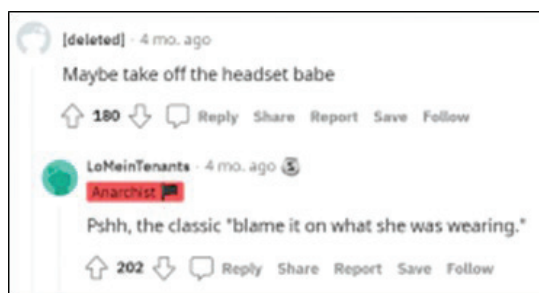


Figure 4. Example of a victim blaming response to sexual violence in the metaverse

Victim blaming also has negative impacts on victims' help-seeking behaviours (Shah, 2021). Victim blaming attitudes within society could lead to self-blame of both online and offline forms of sexual violence by victims and is a critical barrier to disclosure and help-seeking (Campbell, 2006; Jackson, 2021). Additionally, victim blaming attitudes are also associated with a reduced

tendency for others to render support (Koehler & Weber, 2018). Consequently, blaming individuals for being sexual violence victims in the metaverse is of concern as it prolongs their psychological trauma and hinders help-seeking behaviour.

THE IMPLICATIONS OF SEXUAL VIOLENCE IN THE METAVERSE

To mitigate the threat of sexual violence in the metaverse, efforts should be made in the areas of sexuality education and the responsibility for prevention shared among the government, metaverse developers, and parents.

Sexuality Education

While sexual violence in the metaverse is an emerging threat, sexual violence continues to feature more commonly in both offline and online spaces. These unwanted behaviours are usually fuelled by unhealthy, deviant sexual attitudes (Smith, 2016; Sparrow et al., 2020). To counter these unhealthy and deviant sexual attitudes, it is important to ensure youths receive effective sexuality education and character development. Hence, there is a need for upstream sexuality education to promote healthy gender and sexual attitudes early on. Specifically, sexuality education could consider educating youths on respect and consent when interacting with others online (including the metaverse and virtual reality). Youths should also be warned about the dangers of sexual violence in the metaverse, how their virtual behaviours and that of others could impact others in real life, and how to protect oneself when using these technologies.

Shared Responsibility of Policymakers, Industries, and Parents

What policymakers could do

The emerging threat of sexual violence in the metaverse highlights the difficulties that come with monitoring and prosecuting sexual violence in an increasingly online world. Additionally, reviewing the metaverse from a regulatory perspective might be challenging for policymakers as it is currently unclear what the metaverse would look like in the future or if current laws should extend to cover sexual crimes in the metaverse and virtual space.

Currently, the Protection from Harassment Act (POHA) enacted in Singapore in 2014 covers a broad range of anti-social and undesirable behaviours that intentionally cause others harassment, alarm, or distress, including stalking and cyber-bullying. Sexual violence in the metaverse could be considered non-physical insulting communications under the POHA which also has an extra-territorial effect which includes both offenders and victims who may be residing overseas. While the POHA could help in dealing with sexual violence in the metaverse, some victims might believe that the reduction of their experience to a sexual harassment offence does not provide them with the redress they feel they deserve.

Separately, the Ministry of Communications and Information (2022) launched a public consultation in mid-2022 on a proposed Code of Practice for Online Safety (CPOS) where designated social media services are required to have appropriate measures and safeguards to limit the exposure of local users to harmful content. Such proposed safeguards could also potentially be carried over into the metaverse to mitigate the exposure of users – especially children – to sexual content in the metaverse.

What metaverse developers could do

Solely relying on legislation to alleviate sexual violence in the metaverse is inadequate. Metaverse developers have been encouraged to do more in preventing and managing incidents of sexual violence in the metaverse (Sparrow et al., 2020). As more cases of sexual violence in the metaverse emerge, some companies have put in place safety measures (see Table 2). For example, in response to the case of virtual groping in QuiVR, developers created a gesture that players could use to activate a “Personal Bubble” (Stanton, 2016). When activated, any avatar that breaches one’s bubble (i.e., online personal space) disappears out of sight, and the user’s avatar fades away from others’ view as well. This empowers users to create their own safety zone. Other anti-sexual harassment tools that metaverse platforms can consider include allowing users to choose how close other users can get to them before any interactions even occur, as well as giving users easy-access shortcuts to block, mute, and report others (Cortese, 2019). Such tools provide users with agency and empowerment as they have a sense of control over their personal space and gaming experience, without

Table 2. Technological tools to mitigate sexual violence in the metaverse

Year	Metaverse Platforms	Details
2016	<i>AltspaceVR</i>	Space bubble: Users can only come up to about one foot of your avatar before their hands and body disappear from your view
2022	<i>Horizon Worlds and Horizon Venues</i>	Personal boundary: Another user’s forward movement is halted if they come within four feet Safe Zone: Can be activated by a user any time. When activated, nobody can interact with the user in any way until the user lifts the “safe zone”.

being forced to leave the game to avoid virtual sexual violence (Wong, 2016).

What parents could do

Parents could also help their children better protect themselves and establish boundaries with virtual reality and in the metaverse by a) limiting their child’s access where necessary, b) acquiring knowledge about the metaverse and their child’s activities in the metaverse, and c) maintaining communication with their child (see Table 3).

CONCLUSION

Despite the metaverse’s relatively young age, there are increasing reports of sexual violence occurring in the metaverse. While sexual violence in the metaverse is likely to be as endemic as it is on other online platforms, the heightened immersion and realism involved have concerning psychological implications, especially for younger victims. Hence, it is critical for users, educators, parents, and policymakers to act early by putting in place sufficient preventive and responsive measures to mitigate this emerging threat.

Table 3. Tips for parents to help children better protect themselves in the metaverse

Limiting access:	<ul style="list-style-type: none"> • Ensure your child is old enough to be on the metaverse platform/app or uses the device under close supervision • Consider signing out of your metaverse account when not in use
Acquiring knowledge:	<ul style="list-style-type: none"> • Important for parents to be aware of their children’s online activity • Remain informed about the metaverse, virtual reality devices, and the games your child or teen is interested in (including available privacy controls, reporting features, and blocking tools) • Have your child cast their activity in the metaverse onto another phone or laptop screen making it possible for parents to supervise children’s activity (Phippen, 2022).
Maintaining communication:	<ul style="list-style-type: none"> • Have regular conversations with children and teens about their experience in the metaverse and online safety • Talk with your child about the apps being used, potential risks, and what they could do to protect themselves • Educate your child that not everyone in the metaverse may be who they claim to be. • Discuss with your child how to get out of uncomfortable situations. The immersive nature of the metaverse might make it more difficult for youth to leave a situation or conversation. • Reinforce that you are available for support if your child needs help, is upset, or has an uncomfortable experience in the metaverse.

ABOUT THE AUTHORS



Karthigan Subramaniam

is a Psychologist with the Psychological Services Directorate of the Home Team Psychology Division 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.



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 Psychology Division. His research interests are in violent and sexual crimes, offender risk assessment and rehabilitation, scams, and frontline officers' stress and resilience.

REFERENCES

- Allen, C., & McIntosh, V. (2022). Safeguarding the metaverse. *The Institution of Engineering and Technology*. <https://www.theiet.org/media/9836/safeguarding-the-metaverse.pdf>
- Arora, S. (2022, August 5). How the metaverse accelerates economic development for emerging economies. *The Economic Times*. <https://economictimes.indiatimes.com/markets/cryptocurrency/how-the-metaverse-accelerates-economic-development-for-emerging-economies/articleshow/93375549.cms?from=mdr>
- Basu, T. (2021, December 16). The metaverse has a groping problem already. *MIT Technology Review*. <https://www.technologyreview.com/2021/12/16/1042516/the-metaverse-has-a-groping-problem/>
- Campbell, R. (2006). Rape survivors' experiences with the legal and medical systems: Do rape victim advocates make a difference?. *Violence against women*, 12(1), 30-45. <https://doi.org/10.1177/1077801205277539>
- Center for Countering Digital Hate. (2021, December 30). *Facebook's metaverse*. <https://counterhate.com/research/facebooks-metaverse/>
- Christensen, D. (2016). Trauma and touch: Apprehension of touch and relationship quality in survivors of military sexual trauma. *Undergraduate Honors Capstone Projects*, 553. <https://doi.org/10.26076/4572-38f7>
- Cortese, M. (2019, November 2). Designing safer social VR. *Medium*. <https://immerse.news/designing-safer-social-vr-76f99f0be82e>
- Crawford, A. & Smith, T. (2022, February 23). Metaverse app allows kids into virtual strip clubs. *BBC News*. <https://www.bbc.com/news/technology-60415317>
- Easpig, B. N. G., & Humphrey, R. (2016). "Pitching a virtual woo": Analysing discussion of sexism in online gaming. *Feminism & Psychology*, 27(4), 553-561. <https://doi.org/10.1177/0959353516667400>
- Economist Impact (2021). *Global Threat Assessment 2021*. https://safe.menlosecurity.com/https://www.weprotect.org/wp-content/plugins/pdfjs-viewer-shortcode/pdfjs/web/viewer.php?file=https://www.weprotect.org/wp-content/uploads/Global-Threat-Assessment-2021.pdf&attachment_id=&dButton=true&pButton=true&oButton=false&sButton=true#zoom=0&pagemode=none&_wponce=8d4cf849b8
- Franks, M. A. (2017). The desert of the unreal: Inequality in virtual and augmented reality. *UCDL Rev.*, 51, 499. https://repository.law.miami.edu/cgi/viewcontent.cgi?article=1538&context=fac_articles

- Gillespie, E. (2020, December 11). *Virtual rape and sexual abuse: The dangers of immersive technology*. The Feed. <https://www.sbs.com.au/news/the-feed/virtual-rape-and-sexual-abuse-the-dangers-of-immersive-technology>
- Gray, K. L., Buyukozturk, B., & Hill, Z. G. (2017). Blurring the boundaries: Using Gamergate to examine “real” and symbolic violence against women in contemporary gaming culture. *Sociology Compass*, 11(3), e12458. <https://doi.org/10.1111/soc4.12458>
- Hackl, C. (2021, May 2). Defining The Metaverse Today. *Forbes*. www.forbes.com/sites/cathyhackl/2021/05/02/defining-the-metaverse-today/?sh=54dc751b6448
- Internet Watch Foundation (2021, April 21). Campaign launches as new report finds girls at worsening risk of grooming from sexual predators online. <https://safe.menlosecurity.com/https://www.iwf.org.uk/news-media/news/campaign-launches-as-new-report-finds-girls-at-worsening-risk-of-grooming-from-sexual-predators-online/>
- Jackson, G. (2021). Reflections on practice: Experiences of providing care to victims in the Rowan Sexual Assault Referral Centre in Northern Ireland. In *Sexual Violence on Trial* (pp. 22-33). Routledge. https://ebrary.net/174548/law/reflections_practice_experiences_providing_care_victims_rowan_sexual_assault_referral_centre_norther
- Jurgenson, N. (2011). Digital dualism versus augmented reality. *The Society Pages*. <https://safe.menlosecurity.com/https://thesocietypages.org/cyborgology/2011/02/24/digital-dualism-versus-augmented-reality/>
- Koehler, C., & Weber, M. (2018). “Do I really need to help?!” Perceived severity of cyberbullying, victim blaming, and bystanders’ willingness to help the victim. *Cyberpsychology: Journal of Psychosocial Research on Cyberspace*, 12(4). <https://doi.org/10.5817/cp2018-4-4>
- Lavoie, R., Main, K., King, C., & King, D. (2020). Virtual experience, real consequences: The potential negative emotional consequences of virtual reality gameplay. *Virtual Reality*, 25(1), 69–81. <https://doi.org/10.1007/s10055-020-00440-y>
- Lin, J. H. T. (2017). Fear in virtual reality (VR): Fear elements, coping reactions, immediate and next-day fright responses toward a survival horror zombie virtual reality game. *Computers in Human Behavior*, 72, 350–361. <https://doi.org/10.1016/j.chb.2017.02.057>
- Lin, Y. (2020, October 20). *10 virtual reality statistics you should know in 2021 [Infographic]*. <https://Sg.Oberlo.Com/Blog/Virtual-Reality-Statistics>.
- Low, R., & Subramaniam, K. (2022). *The Psychological Impact of Immersive Technology-Facilitated Sexual Violence in the Gaming and Sex Industry* (HTBSC Research Report 03/2022). Home Team Behavioural Sciences Centre.
- McLean, L., & Griffiths, M. D. (2018). Female gamers’ experience of online harassment and social support in online gaming: A qualitative study. *International Journal of Mental Health and Addiction*, 17(4), 970–994. <https://doi.org/10.1007/s11469-018-9962-0>
- Media Literacy Council (2020, October 8). Be Smart: Online Sexual Grooming. <https://www.betterinternet.sg/Resources/Resources-Listing/Be-Smart---Online-Sexual-Grooming>
- Ministry of Communications and Information. (2022, July 13). MCI launches public consultation for proposed measures to enhance online safety for users in Singapore. <https://www.mci.gov.sg/pressroom/news-and-stories/pressroom/2022/7/public-consultation-on-proposed-measures-to-enhance-online-safety-for-users-in-singapore>
- Ng, D. (2022, September 23). Couple say ‘I do’ in Singapore’s first metaverse wedding. *ChannelnewsAsia*. <https://www.channelnewsasia.com/singapore/metaverse-wedding-sandbox-virtual-reality-singapore-first-2960256>
- O’Halloran, K. (2017, October 23). ‘Hey dude, do this’: the last resort for female gamers escaping online abuse. *The Guardian*. <https://www.theguardian.com/culture/2017/oct/24/hey-dude-do-this-the-last-resort-for-female-gamers-escaping-online-abuse>
- Oremus, W. (2022, February 7). Kids are flocking to Facebook’s ‘metaverse.’ Experts worry predators will follow. *The Washington Post*. <https://www.washingtonpost.com/technology/2022/02/07/facebook-metaverse-horizon-worlds-kids-safety/>

Outlaw, J. (2018, April 4). *Virtual harassment: The social experience of 600+ regular virtual reality (VR) users. The Extended Mind*. <https://extendedmind.io/blog/2018/4/4/virtual-harassment-the-social-experience-of-600-regular-virtual-reality-vrusers>

Pallavicini, F., Ferrari, A., Pepe, A., Garcea, G., Znacchi, A., & Mantovani, F. (2018, July). Effectiveness of virtual reality survival horror games for the emotional elicitation: Preliminary insights using Resident Evil 7: Biohazard. In *International Conference on Universal Access in Human-Computer Interaction* (pp. 87-101). Springer, Cham.

Pang, I. (2022, February 16). Sexual assault in the metaverse: Can victims turn to present-day law for justice? *The Home Ground*. <https://thehomeground.asia/destinations/singapore/sexual-assault-in-the-metaverse-can-victims-turn-to-present-day-law-for-justice/>

Park, D. (2022, September 12). S. Korean man sentenced to four years for sexual abuse in metaverse. *Yahoo! Finance*. <https://finance.yahoo.com/news/korean-man-sentenced-four-years-041439436.html>

Patel, N. J. (2021, December 21). Reality or Fiction? *Kabuni*. <https://medium.com/kabuni/fiction-vs-non-fiction-98aa0098f3b0>

Perez, R., & Hazell, C. (2011). *What happens when you touch the body?: The psychology of body-work*. [E-book]. AuthorHouse Publishing.

Petrock, V. (2021, April 15). *US virtual and augmented reality users 2021*. EMarketer. <https://www.emarketer.com/content/us-virtual-augmented-reality-users-2021>

Phippen, A. (2022). Protecting children in the metaverse: it's easy to blame big tech, but we all have a role to play. *Parenting for a Digital Future*. http://eprints.lse.ac.uk/114781/1/parenting4digitalfuture_2022_03_23.pdf

Pinchevsky, G. M., Magnuson, A. B., Augustyn, M. B., & Rennison, C. M. (2019). Sexual victimization and sexual harassment among college students: A comparative analysis. *Journal of Family Violence*, 35(6), 603–618. <https://doi.org/10.1007/s10896-019-00082-y>

Protection from Harassment Act (CAP 256A, 2015 Rev Ed). <https://sso.agc.gov.sg/Act/PHA2014>

Purdy, M. (2022, April 5). How the metaverse could change work. *Harvard Business Review*. <https://hbr.org/2022/04/how-the-metaverse-could-change-work>

Quayle, E., Jonsson, L., & Lööf, L. (2012). Online behaviour related to child sexual abuse: Interviews with affected young people. *ROBERT, Risktaking online behaviour, empowerment through research and training. European Union & Council of the Baltic Sea States*. <https://childrenatrisk.cbss.org/publications/online-behaviour-related-to-child-sexual-abuse-interviews-with-affected-young-people/>

Reeves, C. (2018). The virtual simulation of child sexual abuse: online gameworld users' views, understanding and responses to sexual ageplay. *Ethics and Information Technology*, 20(2), 101-113. <https://doi.org/10.1007/s10676-018-9449-5>

Roper, M. (2022, February 9). Predators use virtual reality chatroom to target children on popular gaming device. *Mirror*. <https://www.mirror.co.uk/news/uk-news/predators-use-virtual-reality-chatroom-26186533>

Rose, J., & Phillips, J. (2022, April 25). Channel 4 Dispatches shows metaverse users boasting that they are attracted to 'little girls aged between the age of nine and 12' and joking about rape and racism in virtual reality online. *The Daily Mail*. <https://www.dailymail.co.uk/news/article-10752287/Channel-4-Dispatches-shows-metaverse-users-boasting-attracted-little-girls.html>

Shah, D. (2021, March 29). *A recap: Violence in a click, a panel discussion on technology-facilitated sexual violence*. Association of Women for Action and Research. <https://www.aware.org.sg/2021/03/a-recap-violence-in-a-click-a-panel-discussion-on-technology-facilitated-sexual-violence/>

- Singh, K. (2022, June 10). There's Not Much We Can Legally Do About Sexual Assault In The Metaverse. *Refinery29*. <https://www.refinery29.com/en-us/2022/06/11004248/is-metaverse-sexual-assault-illegal>
- Slater, M., Antley, A., Davison, A., Swapp, D., Guger, C., Barker, C., Pistrang, N., & Sanchez-Vives, M. V. (2006). A virtual reprise of the Stanley Milgram obedience experiments. *PLoS ONE*, *1*(1), e39. <https://doi.org/10.1371/journal.pone.0000039>
- Smith, I. (2016, October 30). *Even in a virtual world, the harsh reality of sexual harassment persists*. NPR. <https://www.npr.org/sections/alltechconsidered/2016/10/30/499243803/even-in-a-virtual-world-the-harsh-reality-of-sexual-harassment-persists>
- Sparrow, L., Antonellos, M., Gibbs, M., & Arnold, M. (2020). *From 'Silly' to 'Scumbag': Reddit Discussion of a Case of Groping in a Virtual Reality Game* [Online Conference Paper]. Proceedings of the 2020 DiGRA International Conference: Play Everywhere, The Digital Games Research Association. <http://www.digra.org/digital-library/publications/from-silly-to-scumbag-reddit-discussion-of-a-case-of-groping-in-a-virtual-reality-game/>
- Stanton, A. (2016, October 25). *Harassment & superpowers: Dealing with harassment in VR*. UploadVR. <https://uploadvr.com/dealing-with-harassment-in-vr/>
- Sugiura, L., & Smith, A. (2020). Victim blaming, responsabilization and resilience in online sexual abuse and harassment. *Victimology*, *45*–79. https://doi.org/10.1007/978-3-030-42288-2_3
- Suh, A., & Prophet, J. (2018). The state of immersive technology research: A literature analysis. *Computers in Human Behavior*, *86*, 77–90. <https://doi.org/10.1016/j.chb.2018.04.019>
- Thompson, M. P., & Kingree, J. B. (2010). Sexual victimization, negative cognitions, and adjustment in college women. *American Journal of Health Behavior*, *34*(1), 54–59. <https://doi.org/10.5993/ajhb.34.1.7>
- Turchik, J. A., & Hassija, C. M. (2014). Female sexual victimization among college students. *Journal of Interpersonal Violence*, *29*(13), 2439–2457. <https://doi.org/10.1177/0886260513520230>
- Turner, H. A., Finkelhor, D., & Ormrod, R. (2010). The effects of adolescent victimization on Self-Concept and depressive symptoms. *Child Maltreatment*, *15*(1), 76–90. <https://doi.org/10.1177/1077559509349444>
- Waltemate, T., Gall, D., Roth, D., Botsch, M., & Latoschik, M. E. (2018). The Impact of Avatar Personalization and Immersion on Virtual Body Ownership, Presence, and Emotional Response. *IEEE Transactions on Visualization and Computer Graphics*, *24*(4), 1643–1652. <https://doi.org/10.1109/tvcg.2018.2794629>
- Wiederhold, B. K. (2022). Sexual harassment in the metaverse. *Cyberpsychology, Behavior, and Social Networking*, *25*(8), 479–480. <https://doi.org/10.1089/cyber.2022.29253.editorial>
- Wang, D., Guo, Y., Liu, S., Zhang, Y., Xu, W., & Xiao, J. (2019). Haptic display for virtual reality: progress and challenges. *Virtual Reality & Intelligent Hardware*, *1*(2), 136–162. <https://doi.org/10.3724/sp.j.2096-5796.2019.0008>
- Wong, J. C. (2016, October 26). Sexual harassment in virtual reality feels all too real – 'it's creepy beyond creepy'. *The Guardian*. <https://www.theguardian.com/technology/2016/oct/26/virtual-reality-sexual-harassment-online-groping-quivr>
- Wong, Y., & Haciyakupoglu, G. (2022, June 13). Southeast Asia Must Be Wary of Gendered Cyber Abuse. *The Diplomat*. <https://thediplomat.com/2022/06/southeast-asia-must-be-wary-of-gendered-cyber-abuse/>
- Yokoi, T. (2021, March 4). Female Gamers Are On The Rise. Can The Gaming Industry Catch Up? *Forbes*. <https://www.forbes.com/sites/tomokoyokoi/2021/03/04/female-gamers-are-on-the-rise-can-the-gaming-industry-catch-up/?sh=5df2398af9fe>
- Yuan, N. P., Koss, M. P., & Stone, M. (2006). The psychological consequences of sexual trauma. *VAWnet, a Project of the National Resource Center on Domestic Violence*. <https://vawnet.org/material/psychological-consequences-sexual-trauma>

CYBER SEXTORTION: WHO'S REALLY BEHIND THE WEBCAM?

Tan Wei Liang, Carolyn Misir & Jansen Ang
Police Psychological Services Department, Singapore Police Force

ABSTRACT

The rising prevalence of cyber sextortion in Singapore is an imminent issue that warrants our attention. However, there is a dearth of research regarding cyber sextortion, especially with regards to webcam blackmail. This paper aims to address this gap by shining a light on the modus operandi of cyber sextortion, the psychosocial factors involved in the various stages, and the challenges involved in combating it. A comprehensive literature review reveals that webcam blackmail is carried out by transnational cyber sextortion offenders who operate as part of organised crime syndicates based mainly in the Philippines, Morocco, or the Ivory Coast. They tend to target victims in countries where English is a primary Internet language in both Asia (e.g., Singapore, Hong Kong) and the West (e.g., United States, United Kingdom) through a four-stage process. According to routine activity theory, the formation of cyber sextortion crime syndicates can be explained by convergence settings that facilitate co-offending. Similarly, routine activity theory can also account for the victimology of cyber sextortion victims – those with higher usage of social media have higher victimisation risk. Lastly, the main challenges in combating cyber sextortion include victim's reluctance to report crime, secrecy surrounding cyber response capabilities, and the problem of attribution. Future research directions will be discussed.

WHAT IS CYBER SEXTORTION?

Cyber sextortion is defined as “the threat to distribute intimate, sexual materials online unless a victim complies with certain demands” (O'Malley & Holt, 2020). The use of explicit images to manipulate victims over online platforms distinguishes cyber sextortion from traditional extortion (Jacobs & Franks, n.d.). Cyber sextortion is under an overarching spectrum of image-based sexual abuse (IBSA), consisting of crimes such as revenge pornography and non-consensual sexting, in which explicit images are used for harm (Powell et al., 2019). The power and control an offender wields over the victim to possibly harm, and therefore threatening total compliance, is the crux of sextortion (O'Malley & Holt, 2020).

The methodology and motivations that fuel cyber sextortion are similar to other interpersonal crimes such as intimate partner violence (Bates,

2016), cybercrime (National Crime Agency, 2018), and child exploitation (Acar, 2016). However, there are three distinct differences between cyber sextortion and other interpersonal crimes: cyberspace, possession, and extortion (Acar, 2016). Firstly, the victim and perpetrator of cyber sextortion may have never met or interacted physically, and the crime is solely committed online. Secondly, the offender possesses compromised images of the victim regardless of how they were produced or obtained (Acar, 2016), although it tends to be through non-consensual means such as manipulation or coercion (Liggett, 2019). Lastly, the victim is coerced into acts through threats to disseminate images, and the acts could be sexual, behavioural, or financial in nature (Acar, 2016).

Cyber sextortion offenders are a heterogeneous group of individuals that vary in target victim, modus operandi, demands, and motives (O'Malley

Table 1. Typology of Cyber Sextortion Offenders

	Minor-Focused	Cybercrime	Intimately Violent	Transnational Criminal
Target Victim	Minors (less than 18 years old), strangers, distinct gender preference	Strangers, predominantly female	Former or current romantic partners, female	Strangers, male, preferably rich, married, or religious
Modus Operandi	Impersonation and psychological grooming	Theft/hacking, social engineering scams, harassment tactics	Threaten using sexually explicit materials obtained during the relationship	Impersonation and deception
Demands	Sexually explicit materials, physical sexual conduct	Sexually explicit materials, money	Remain in relationship, end relationship with others, leave their work, meet the offender	Money
Motivation	Sexual interest in minors	Sexual pleasure/ financial	Control the victim's behaviour	Financial

& Holt, 2020). According to O'Malley and Holt (2020), there are four distinct types of cyber sextortion offenders:

- (i) minor-focused cyber sextortion offenders,
- (ii) cybercrime cyber sextortion offenders,
- (iii) intimately violent cyber sextortion offenders, and
- (iv) transnational criminal cyber sextortion offenders.

The Four Types of Cyber Sextortion Offenders

Minor-Focused Cyber Sextortion Offenders

Minor-focused cyber sextortion offenders tend to have a distinct gender preference when it comes to victims under 18 years of age. A recent study by O'Malley and Holt (2020) found that 71.3% of the offenders exclusively targeted female minors, 20% targeted only male minors, and only 7.5% offenders targeted both genders. This is consistent with studies that differentiate between preferential child sexual offenders who target children with specific characteristics (i.e., specific age and gender) and non-preferential offenders who target a wide range of children based on opportunity (Knight & Prentky, 1990; Lanning, 2010). Such sextortion offenders are more likely

to target strangers and demand sexually explicit material or physical sexual contact. The majority of these offenders utilise some form of grooming to manipulate minors into self-generating sexual images. As part of the grooming process, they may impersonate as similar-aged peers to seduce minors and fabricate a sense of trust, which in turn lead to victims being more receptive to mutual image-sharing (O'Malley & Holt, 2020). Furthermore, online conversations gradually evolve from flattering to sexually explicit language, slowly grooming the victim towards increasingly sexually explicit performance (Acar, 2016; Kopecký et al., 2015). Lastly, minor-focused cyber sextortion offenders might be motivated by a sexual interest in minors. O'Malley and Holt (2020) found that approximately 55% of those arrested had large collections of child sexually abusive materials, which long-term use had been found to be significantly associated with sexual interest in children (Seto & Eke, 2017) and sexual recidivism (Eke et al., 2019; Seto & Eke, 2015). However, this motivation cannot be generalised across all minor-focused offenders as some simply target minors due to ease of access and manipulation (O'Malley & Holt, 2020).

Cybercrime Cyber Sextortion Offenders

Cybercrime cyber sextortion offenders use computer-based tactics to acquire images and demand sexual material or contact from victims, who are predominantly female strangers (O'Malley & Holt, 2020). Most cybercrime cyber sextortion offenders use theft/hacking to illegally obtain intimate images of victims, while others use harassment tactics or social engineering scams. Although the use of hacking reflects the technological nature of cyber sextortion, the majority of such cases do not involve technologically advanced or specialised knowledge. For example, many offenders use social engineering tactics or research victims' online presence to guess their account passwords. A smaller proportion of the more technologically sophisticated offenders obtain the compromised images through hacking the victims' webcams, distributing malware to the victims, or launching ransomware attacks whereby victims are locked out of their accounts until they comply with the offender's demands (O'Malley & Holt, 2020).

Intimately Violent Cyber Sextortion Offenders

Intimately violent cyber sextortion offenders target former or current romantic partners and use cyber sextortion to manipulate victim behaviour. Their victims tend to be exclusively female (O'Malley & Holt, 2020). The majority of such offenders demand nonsexual behaviours from victims such as remaining in romantic relationships with them, ending new relationships with others, leaving their current work, or continue staying in contact with them (O'Malley & Holt, 2020). Intimate partner cyber sextortion is relatively similar to revenge pornography (Citron & Franks, 2014), but they differ in their emphasis. The former relies on the threat to distribute images to control behaviour, regardless of whether images are ultimately distributed, while the latter focuses on the distribution itself.

Transnational Criminal Cyber Sextortion Offenders

Transnational criminal cyber sextortion offenders employ scams to trick victims into producing explicit images or videos, before utilising them to demand money, exploiting the victims' feelings of shame and embarrassment to manipulate

them into compliance (O'Malley & Holt, 2020). A common example is the webcam blackmail in which offenders seduce victims to engage in sexually explicit video chats and record the sexual acts for subsequent extortion. Some offenders use pre-downloaded webcam sessions or pre-recorded video from pornographic websites to trick the victim into believing the encounter is real (CNA, 2019; O'Malley & Holt, 2020). These offenders target strangers and show no preference in terms of victim age although they tend to only target males and have a preference for men who are successful (O'Malley & Holt, 2020), religious, or married (O'Neill et al., 2016) as they are more likely to comply with their demands. Transnational criminal cyber sextortion offenders are distinct from other cyber sextortionists as (i) they are part of crime syndicates engaged in crime as a business or for profit, (ii) their demands are strictly financial, (iii) they specifically target men, and (iv) their offenses progress rapidly with time-sensitive demands, which result in heightened sense of urgency for the victims (O'Malley & Holt, 2020). Lastly, these crime syndicates mostly operate in the Philippines, Morocco, and the Ivory Coast (Ryan, 2018; Whitworth, 2018).

CYBER SEXTORTION IN SINGAPORE

Cyber sextortion, in the form of webcam blackmail, is on a rising trend globally (UNODC, 2020). According to the United Kingdom (UK) National Crime Agency (2018), the number of UK sextortion victims has risen threefold in just two years, from 428 in 2015 to 1,304 in 2017. In Malaysia, a total of 23 cyber sextortion cases were reported to CyberSecurity Malaysia between March and April 2020, compared to 15 in 2019 and 6 in 2018 during the same period (Yuen, 2020). In Singapore, cyber extortion cases increased from 68 in 2019 to 245 in 2020, and more than \$793,000 was lost as a result in 2020 alone (Today, 2021).

There are several reasons for the rise in cyber sextortion cases in Singapore. Firstly, with Singapore having a high internet penetration of 90% and an overwhelming 84.4% of the population being social media users (Kemp, 2021), it is unsurprising that technology-enabled crimes such as cyber sextortion have surged over the past few years. Since cyber sextortionists prowl through the internet for potential victims,

especially on social media platforms (Singapore Police Force, 2020), the high internet and social media usage among Singaporeans provide a large potential pool of victims. This is facilitated by the global connectivity and anonymity afforded by the internet which allow cyber sextortionists to easily target victims globally at a relatively low risk (Gordon et al., 2000).

Secondly, English is the predominant language used in Singapore, hence language is not a barrier for transnational criminals (Phoebe, 2017). This is supported by the fact that transnational cyber sextortionists generally operate between countries with a common language and they preferentially target countries with English as a primary internet language (EUROPOL, 2017). Thirdly, financially motivated cyber sextortionists tend to target successful men with good careers (CNA, 2019; O'Malley & Holt, 2020) and Singapore having the highest proportion of highly skilled workers in the Asia Pacific (World Economic Forum, 2015) presents an attractive target. Lastly, Singapore may also be targeted simply because of similarity in time zone with the Philippines, where cyber sextortion crime syndicates mainly operate (Parry, 2017).

Cyber sextortion is thus an issue in Singapore that warrants attention. This article focuses on the transnational criminal cyber sextortion offenders who are the main culprits behind the rising trend of cyber sextortion, particularly webcam blackmail, in Singapore.

THE FOUR STAGES OF CYBER SEXTORTION

We propose a model to explain cyber sextortion consisting of four stages, namely fake profile creation, victim hunting, victim grooming, and blackmailing (Figure 1). This model is primarily based on interviews with transnational cyber sextortionists who operate in the Philippines (CNA,

2019), as well as relevant academic literature and news sources.

Stage 1: Fake Profile Creation

Catfishing is a common method used by sextortionists (Carlton, 2020) and it refers to the creation of fake online profile for deceptive purposes (Harris, 2013). It primarily serves two functions for the sextortionists: to entice and befriend victims, as well as to hide the offender's identity. Sextortionists will create fake profiles, usually posing as attractive women, on social media platforms such as Facebook or dating apps like Tinder and OkCupid (Carlton, 2020; Paul, 2019; Singapore Police Force, 2020). They will try to make the account look as real as possible to gain the victim's trust (CNA, 2019). For example, sextortionists using social media sites such as Facebook will do regular updates to increase its legitimacy (CNA, 2019). To make it more convenient for them to do so, they will usually "clone" someone else's account (CNA, 2019; Flynn, 2015). In other words, their profiles will be identical to another legitimate user's profile in most aspects such as display picture, uploaded photos, and status updates.

Stage 2: Victim Hunting

Using the fake profiles they have created, sextortionists start hunting for victims on online social networking platforms, predominantly on Facebook (CNA, 2019; Ryan, 2018). Facebook is the ideal platform for the sextortionists as it encapsulates almost everything they need – befriend function, video chat function, and personal details of potential victims such as photographs and list of loved ones (CNA, 2019). They typically search for their victims on Facebook through keywords that reflect the characteristics they are seeking for in their victims (e.g., Engineers living in Singapore; CNA,

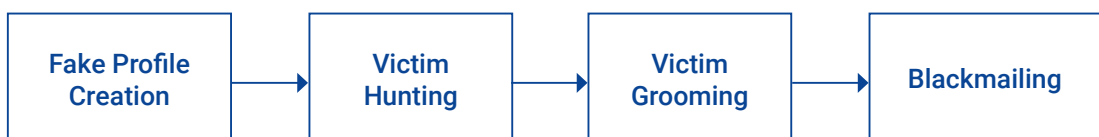


Figure 1. The Proposed Model of Cyber Sextortion

2019). Sextortionists prefer to target men who are successful, religious or married. In addition, they prefer victims who have made a lot of their personal information publicly available on their Facebook profile, especially regarding their family and relationship status, so they have easier access to useful information for subsequent blackmailing (CNA, 2019). Lastly, sextortionists tend to preferentially target countries where English is a primary internet language, such as the United Kingdom, United States, Australia, Singapore, Hong Kong, Indonesia and Malaysia (EUROPOL, 2017). Once the sextortionists have found their potential victim, they will befriend and initiate conversations with them (CNA, 2019).

Stage 3: Victim Grooming

During the conversation, the sextortionists attempt to groom the victim by sending increasingly sexually suggestive messages and try to get intimate with them (Carlton, 2020; Stebbins, 2021). Once the victim appears to be romantically interested, the sextortionists will suggest moving the interaction to a telecommunication platform that enables video chat such as Skype and tries to manipulate the victim into engaging in sexually explicit video chats (Ryan, 2018; Stebbins, 2021). Pre-downloaded webcam sessions or pre-recorded videos from pornographic websites are sometimes used to trick the victim into believing the encounter is real (CNA, 2019; O'Malley & Holt, 2020). In such video chats, the victim is asked to perform compromising sexual acts which, unknown to them, are being recorded by the sextortionists (Carlton, 2020; Singapore Police Force, 2020). It is important for the sextortionists to capture the victim's face and genitals in the recordings to enhance the threat for subsequent blackmailing (O'Neill et al., 2016). This entire process usually occurs within a relatively short period of approximately 30 minutes (Parry, 2017).

Stage 4: Blackmailing

Sextortionists will gather the victim's personal information through the victim's social media profile and record their list of family members and friends (CNA, 2019; Stebbins, 2021). Some sextortionists may even conduct a public record search on their victims to find their address

and employer (Stebbins, 2021). Once the sextortionists have enough information, they will threaten their victims into complying with their financial demands to prevent the release of their compromised videos (Carlton, 2020; O'Malley & Holt, 2020; Singapore Police Force, 2020). There have also been known cases of sextortionists using compromising photographs that the victims have shared with them or doctored photographs taken from victims' social media accounts to threaten the victims instead (Singapore Police Force, 2020). Once the victims start paying, the sextortionists will never stop threatening and demanding for more money (CNA, 2019; Whitworth, 2018).

PSYCHOSOCIAL FACTORS INVOLVED IN CYBER SEXTORTION

Throughout the cyber sextortion process, there are various psychosocial factors which influence both the offender and the victim. These factors are further elaborated in detail according to the proposed four-stage model of cyber sextortion.

Stage 1: Fake Profile Creation

According to Jaishankar (2008), identity flexibility and dissociative anonymity in cyberspace facilitate cybercrimes. It is difficult to determine the real identities of people on the internet as they can choose to hide or alter their identities (Suler, 2004). This is evident from the usage of fake online profiles by sextortionists. This anonymity is one of the principal factors resulting in the online disinhibition effect which empowers people to act out and express themselves freely in cyberspace (Suler, 2004). Anonymity may also lead to de-individualisation in which one loses one's sense of individuality and personal responsibility, and this is one of the main reasons for cyberspace deviance (Demetriou & Silke, 2003). When individuals have the opportunity to separate their actions from their real time world and identity, it creates a false sense of safety from the repercussions of their actions (Jaishankar, 2008). In such a dissociation process, they may feel that they do not have to take full responsibility for their words said or actions taken in anonymity since it cannot be directly associated with them (Suler, 2004). In fact, people may even convince themselves that such

behaviours “aren’t me at all” (Suler, 2004, p. 322). Hence, by assuming a false identity, sextortionists can morally disengage themselves from their deceptive and coercive behaviour.

Using photos of attractive women as their display picture works in favour of the sextortionists in two ways. Firstly, physical attractiveness stereotype may come into play which biases the victim’s perception of the offender. Physical attractiveness stereotype is a tendency to associate physically attractive people with the possession of socially desirable personality traits (Dion et al., 1972). Studies have found that physically attractive people are perceived to be more trustworthy (Shinners & Morgan, 2009; Zhao et al., 2015) and people tend to disclose more intimately to others who are physically attractive (Brundage et al., 1976). This implies that if the victims perceive the offenders to be trustworthy based on their attractive display pictures, they will be more likely to fall for their ruse, facilitating the offenders’ commission of crime. Secondly, pictures of attractive women may serve as visceral sexual cues which influence the victim’s subsequent behaviour. Visceral cues promote rapid processing of information based on intuitive feelings and reduce people’s motivation to process information carefully (Lea et al., 2009; Norman, 2002). Indeed, studies have found that visceral sexual cues led to lower sensitivity to risk information, which in turn increases risk-taking propensity for both sexual and non-sexual behaviours (Ditto et al., 2006; Skakoon-Sparling et al., 2016). This implies that the usage of attractive photos by the sextortionists may lead to visceral processing of the victims, which in turn increases the likelihood of risky online behaviours, such as engaging in sexually explicit video chat with a stranger.

Stage 2: Victim Hunting

According to rational choice theory (Clarke & Cornish, 1985), offenders will perform a cost-benefit analysis before determining whether it is worth committing a crime; crime is more likely to occur if the perceived benefits are high and the perceived costs are low (Piquero & Hickman, 2002). Cybercriminals are no exception (Modarres et al., 2013; Wright, 2010).

There are few ‘costs’ to cyber sextortion since it can be easily carried out with just an internet

connection and moderate proficiency in English (Parry, 2017). The only perceived costs are likely to be the amount of time invested and the risk of getting apprehended. The former cost can be minimised by targeting victims in the same time zone so as to reduce communication delays (Yu et al., 2016) and the latter can be minimised by targeting overseas victims using a false identity which complicates investigation (Gercke, 2014). This may explain why cyber sextortionists prefer targeting overseas victims in the same time zone (Parry, 2017).

Specifically, cyber sextortionists target men who are successful, religious or married to maximise perceived benefits in terms of a higher likelihood of successful extortion. These characteristics of victims make them uniquely vulnerable in one way or another. Firstly, successful people are likely to be targeted due to their greater financial capacity to pay the ransom. Not only are they able to afford a higher amount, they are also more likely to pay as they have a reputation to uphold. Secondly, religiosity is positively associated with both viewing oneself as moral (e.g., Furrow et al., 2004; Walker et al., 2012; Johnston et al., 2013; Vitell et al., 2009) and impression management (meta-analytic $r = 0.31$; Sedikides & Gebauer, 2010), which refers to an individual’s efforts to influence others to view them as moral. Hence, religious people might be particularly sensitive to information that threatens their moral self-image (Ward & King, 2018). The act of engaging in sexually explicit video chat with a stranger is likely to be deemed as “immoral” and unacceptable by societal norms. Consequently, victims who are religious will be especially concerned about tarnishing their moral self-image if their compromised videos are disseminated and hence, more likely to comply with the demands of the sextortionists. Thirdly, the act of engaging in sexually explicit chat with an opposite gender could be considered an act of sexual infidelity if one is married, and such act is widely deemed to be immoral and unacceptable within marriage (McKeever, 2020; Van Hooff, 2017). This implies that married victims are likely to suffer from dire marital repercussions if their partners find out about it and may even face hostility from society with the recent hardening of attitudes towards infidelity (Van Hooff, 2017). Therefore, this additional relational cost is

likely to make married men more vulnerable to blackmailing by the sextortionists.

Stage 3: Victim Grooming

Cyber sextortionists tend to sexually escalate the conversation by using sexual language shortly into the conversation (Ryan, 2018; Stebbins, 2021). Indeed, online grooming involves a greater usage of direct sexual solicitation compared to offline grooming, mainly in the form of desensitisation talk (Lorenzo-Dus et al., 2016). This is likely due to the higher number of interpersonal barriers in physical settings and the absence of nonverbal cues in online settings mitigates some of those barriers (McKenna & Bargh, 1999), resulting in greater usage of direct solicitation to achieve intimate levels of interpersonal communication. This grooming process does not necessarily occur over a long period – for example, online grooming of children can happen in as little as 18 minutes (Lorenzo-Dus & Izura, 2016).

Cyber sextortionists exploit the victims' psychoemotional vulnerabilities such as desire and self-value to manipulate them into complying with their requests (Sinnamon, 2017). Firstly, desire along with the perception of a lack of means to obtain it makes an individual vulnerable to the manipulations of anyone who is able to grant it (Sinnamon, 2017). Sextortionists prey on sexual desires or simply desires for companionship. They tend to converse in a way that tricks their victims into believing they are romantically interested in them and would like to engage in sexual intimacy, luring them into a "honeytrap". Secondly, low self-esteem, self-worth, and self-efficacy are amongst the most vulnerable dispositions open to exploitation by others (Sinnamon, 2017). Individuals with low self-esteem are vulnerable to the actions of people who can give them a sense of value (Sinnamon, 2017). Hence, as long as the sextortionists are able to make the victims feel good about themselves, it is easier to manipulate them into increasingly higher levels of sexual behaviour over time (Sinnamon, 2017). Indeed, Ireland and colleagues (2015) have found that lower self-esteem is likely to increase a person's vulnerability for sexual exploitation, although the causality direction remains unclear.

Generally, sextortionists use sweet-talking tactics (Powell, 2021). However, even by simply posing as

attractive women and showing romantic interest in the victims will also make the victims feel good about themselves as self-esteem is positively associated with self-perceptions of desirability as a mate (Pass et al., 2009). This vulnerability will in turn make the victims highly susceptible to losing themselves and become increasingly willing to do whatever is asked of them in return for the attention given by the sextortionists (Sinnamon, 2017).

Stage 4: Blackmailing

Blackmailing involves the use of threat to induce fear in the victims with the aim of getting them to comply with the sextortionist's demands. Unfortunately, most victims do end up complying (Parry, 2017). This may be accounted for by two reasons. Firstly, fear may trigger worry, which in turn results in impaired cognitive function (Zhuang et al., 2016) and subsequently poor decision-making (Zamarian et al., 2011). For example, when the sextortionists threaten to disseminate the victims' compromised videos, fear will arouse and the victims will start to worry about the potential repercussions if their videos are disseminated. This will in turn affect their ability to think carefully (impaired cognitive function) and result in them simply paying the sextortionists without considering better alternatives (poor decision-making).

Secondly, according to the stage model of processing of fear-arousing communications (Das et al., 2003; De Hoog et al., 2005), individuals who perceive both the severity of threat and their own vulnerability to be high will be in a defence motivation state (De Hoog et al., 2008). This is likely to be the case for cyber sextortion victims since they are preferentially selected by sextortionists due to their greater vulnerability – for example, successful, married, or religious people are prime victim targets since they have more to lose if their compromised videos are disseminated. Defence-motivated individuals tend to have positive bias in the processing of a threat-mitigation strategy, and consequently heightened motivation to engage in it, regardless of the quality of justifications supporting such action (De Hoog et al., 2008). In the context of cyber sextortion, the threat-mitigation strategy salient to the victims tends to be paying the sextortionists to nullify the threat. Victims might engage in a biased search

for arguments to justify their action of paying the sextortionists and eventually succumb to it.

However, once the victims start paying, the sextortionists will not stop demanding more (CNA, 2019; Whitworth, 2018). Despite this, some victims still choose to comply with the repeated demands. This is likely due to sunk cost fallacy whereby investment of money, effort, or time increases one's tendency to continue a course of action (Arkes & Blumer, 1985). The victims may think that since they have already paid the sextortionists a sum of money, they have to continue paying to ensure the non-disclosure of their compromised videos, otherwise, their previous payment would be wasted.

ROUTINE ACTIVITY THEORY & CYBER SEXTORTION

Routine activity theory provides an account of how opportunities for crime arise through the daily routines of one's social interaction (Cohen & Felson, 1979), postulating that crime is likely to occur when three essential elements of crime converge in space and time: a motivated offender, a suitable target, and the absence of capable guardianship (Cohen & Felson, 1979). Although the theory was originally developed to explain macro-level changes in crime levels through changes in people's routine activities, it has subsequently been applied at an individual level to account for variation in individual risk of victimisation (Tewksbury & Mustaine, 2010). Routine activity theory is not only useful for explaining victimology, but also the rise of organised crime, including the formation of cyber sextortion crime syndicates based overseas and the victimology of cyber sextortion in Singapore.

Formation of Cyber Sextortion Crime Syndicates

One of the most prolific transnational criminal cyber sextortion offenders is a woman by the name of Maria Caparas, who is believed to have pioneered the webcam blackmail and operates a cyber sextortion ring in the Philippines (CNA, 2019; O'Malley & Holt, 2020). Her crime syndicate mainly operates within North Hills, a remote village in the Bulacan district (Parry, 2017). This is likely because Maria Caparas lives in North Hills,

making it much more likely for her to converge with potential co-offenders within this community and to recruit them. In other words, this village itself has become an offender convergence setting. Such offender convergence setting provides a stable and predictable source of co-offenders, which helps to mitigate the potential individual, group, or network instabilities in crime syndicates (Felson, 2003). Currently, it is estimated that about 70% of the 1,500 households in the village are making their living through cybercrime under her leadership (Parry, 2017).

Victimology of Cyber Sextortion

Drawing from both routine activity theory (Cohen & Felson, 1979) and lifestyle exposure theory (Hindelang et al., 1978), Reyns et al. (2011) have developed a cyberlifestyle-routine activity theory with four main components: i) exposure to motivated offenders, ii) proximity to motivated offenders, iii) target attractiveness, and iv) guardianship. According to the theory, the combination of these four concepts results in the presence of opportunity for cybercrime to occur.

For cybercrime, *exposure to motivated offenders* is assessed in terms of digital actions such as the amount of time spent online, the number of media posted online, or the amount of personal information shared (Henson, 2020; Reyns et al., 2011). Essentially, the larger an individual's digital fingerprint, the more exposed one is to potential offenders (Henson, 2020). Since there is no physical contact in cyberspace, *proximity to motivated offenders* is assessed by virtual proximity – extent of virtual interactions potential victims may have with offenders (Henson, 2020; Reyns et al., 2011). This may include factors such as whether an individual accepts friend or follow requests on their social networking platforms from strangers and the number of friends an individual may have on those platforms (Henson, 2020; Reyns et al., 2011). Essentially, the more frequent an individual puts themselves in potentially dangerous situations, the more likely they will be targeted by offenders (Henson, 2020). Generally, both concepts imply that the higher the social media usage, the higher the risk of victimisation. This means that Singapore is particularly vulnerable, as not

only does Singapore have a high proportion of social media users (i.e., 84.4%; Kemp, 2021), the number of social media users and the average time Singaporeans spent on social media have been growing exponentially over the years (Koh, 2021). This could partially account for the rising number of cyber sextortion victims in Singapore as Singaporeans are more likely to be exposed to and targeted by the offenders.

Target attractiveness is influenced by a myriad of factors – the ease with which someone may be approached by a potential offender, the meaning the person has for an offender, and/or the amount of information available about the person (Henson, 2020; Reyns et al., 2011). Generally, the key factors determining online target attractiveness are perceived vulnerability and information availability. It may be measured by examining the amount or type of personal information an individual posts online (e.g., relationship status, contact information, photos/videos, etc). Essentially, the more information that can be accessed about an individual online, the more attractive that individual becomes (Henson, 2020). However, Singaporeans are generally very concerned about their data security (Singapore Business Review, 2020) and are uncomfortable with sharing data on their social media (Heo, 2021). Therefore, Singaporeans are unlikely to be targeted due to information availability but other factors such as economy prosperity and common language as explained previously.

Lastly, *guardianship* is a central component of routine activity theory and it can be analysed in terms of both physical and social guardianship (Henson, 2020). Physical guardianship often involves target hardening, such as the presence of firewalls and security programmes (Choi, 2008; Holt & Bossler, 2008), whereas social guardianship refers to the presence of others, whose mere presence may discourage crime from happening (Felson, 1995), such as the presence of parents or guardians to monitor one's internet activity (Reyns et al., 2011). However, with respect to the crime of cyber sextortion, these protections are unlikely to be effective. Online physical guardianship is meant to protect the computer from external threats and not protect the user against potentially unwanted communications. Similarly, online social guardianship is unlikely to

be relevant as most victims of cyber sextortion are adult working males who are unlikely to have their internet activity monitored by others. Therefore, the presence of capable guardianship may not be as applicable in the victimology of cyber sextortion.

CHALLENGES IN COMBATING CYBER SEXTORTION

Victim's Reluctance to Report Crime

There is a huge problem of under-reporting of cybercrimes. The FBI's Internal Crime Complaint Center (IC3) estimated in 2016 that only 15% of cybercrime victims report their crimes to law enforcement. According to Kidd & Chayet (1984), the three main factors which result in non-reporting are: i) victim fear, ii) feelings of helplessness and the perceived powerlessness of police, and iii) the fear of further victimisation.

Victims of cyber sextortion are afraid that the sextortionists will either forward their compromised videos to their loved ones or upload them online. This fear, compounded by the tight payment deadline given by the sextortionists, may compel victims to just pay the ransom instead of reporting to the police. Crime victims commonly perceive themselves to be helpless and may view agents of the criminal justice system in the same way. The loss of felt competence that accompanies the inability to control outcomes may spread to the victim's view of others, including the criminal justice system (Kidd & Chayet, 1984). In other words, if the victims feel helpless, then they may suspect the criminal justice system can offer little to help too. This may be especially true for cybercrimes such as cyber sextortion in particular as it is often unclear to victims how law enforcement will provide any significant assistance in terms of stopping the threat of exposure, recovering data, or stopping explicit material from being shared online (Wolff, 2018). Hence, victims may not feel the need to report to the police. Lastly, following victimisation, an individual may wish to avoid further trauma by avoiding, excluding, or eliminating contact with any persons or organisations that might traumatise them (Berg & Johnson, 1979). Sometimes, this may include the police since, for cyber sextortion cases, victims are already embarrassed by their

own actions and do not want to show the police their compromised videos for investigation purposes. Furthermore, statement-taking may inadvertently cause the victims to relive the entire humiliating experience again. All these are psychological costs which further contribute to the victim's personal suffering.

However, this reluctance to report cyber sextortion poses a major problem in three aspects: i) difficulty in obtaining data for research purposes (Jurecic et al., 2016); ii) downplaying the prevalence of the crime which may result in insufficient resources being allocated to combat such crime (Wolff, 2018); iii) sextortionists tend to be prolific repeat offenders (Jurecic et al., 2016) so underreporting may potentially snowball to many more victims.

Obstacles Hindering Deterrence of Cybercrime

Deterring financially motivated cybercrime, such as cyber sextortion, relies mainly on concepts of deterrence or dissuasion by denial (Goldman & McCoy, 2016), which is "deterring an action by having the adversary see a credible capability to prevent him from achieving potential gains adequate to motivate the action" (Davis, 2014, p. 2). This approach is useful for reducing the threat from cybercrime as it explicitly focuses on diminishing the anticipated benefits of action.

Attribution is crucial for deterrence as deterrence is fundamentally about communication and a deterrent message can only be appropriately communicated when it is clear who the recipient should be (Goldman & McCoy, 2016). Without confidence in attribution, a cybercrime victim cannot convince potential offenders that their actions will have repercussions. However,

attributing cybercrimes to their perpetrators with a high degree of confidence remains a challenge. This is especially so for transnational cyber sextortion with the offenders assuming a false identity and being based overseas. This increases tracking difficulties and consequently, hinders crime deterrence.

CONCLUSION

In recent years, the number of cyber sextortion cases has been rising in Singapore, and it is a cause for concern that warrants attention. Hence, this study seeks to contribute to the limited literature on cyber sextortion, particularly with regards to webcam blackmail. It does so by proposing a four-stage model of cyber sextortion comprising fake profile creation, victim hunting, victim grooming, and blackmailing, as well as the underlying psychosocial factors involved in each of these stages. Findings suggest that cyber sextortionists are mainly operating as part of transnational organised crime syndicates based in the Philippines, Morocco, and the Ivory Coast, and they tend to target victims from countries with English as a primary Internet language, such as Singapore. The formation of such crime syndicates and the victimology of cyber sextortion can be explained by the routine activity theory. Lastly, the challenges of combating cyber sextortion have also been highlighted. Although this study is mainly exploratory, it can serve as a foundation for future research in cyber sextortion. Future studies can build upon this study to empirically validate the reliability of the findings or examine in greater detail wider demographics of transnational cyber sextortionists to further refine the proposed model. Future studies could also look into data analysis of reports lodged to validate this proposed model of cyber sextortion.

ABOUT THE AUTHORS



Tan Wei Liang

was a research intern with the Operations and Forensic Psychology Division of the Police Psychological Services Department. He graduated from the National University of Singapore with a Bachelor of Arts (Hons) in Psychology and completed his Master's degree in Investigative and Forensic Psychology at the University of Liverpool. Broadly speaking, he is interested in crimes and psychological research.



Carolyn Misir

is a principal psychologist in the Operations and Forensic Psychology Branch (OFP) of the Singapore 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-related areas of the work in OFP while concurrently building deep domain expertise and research in the areas of investigative and criminal psychology. She is concurrently also a principal psychologist in the area of forensic psychology at Centre of Advanced Psychological Sciences (CAPS) where she specialises in crime-related research.



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 & 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, Jansen 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 organisational excellence in the police. He is also the Police's representative on the National CARE Management Committee that is the body responsible for managing the psychological impact arising from national crises and incidents. An Associate Professor (Adjunct) at the Nanyang Technological University in Singapore, he lectures on the psychology of crisis stress at the College of Humanities and Social Sciences. His 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

Acar, K. V. (2016). Sexual Extortion of Children in Cyberspace. *International Journal of Cyber Criminology*, 110-126. doi:10.5281/zenodo.163398

Arkes, H. R., & Blumer, C. (1985). The Psychology of Sunk Cost. *Organizational Behavior and Human Decision Processes*, 35(1), 124-140. doi:10.1016/0749-5978(85)90049-4

Bates, S. (2016). Revenge Porn and Mental Health: A Qualitative Analysis of the Mental Health Effects of Revenge Porn on Female Survivors. *Feminist Criminology*, 12(1), 22-42. doi:10.1177/1557085116654565

Bechlvaniadis, C., Lagnado, D. A., Zemla, J. C., & Sloman, S. (2017). Concreteness and abstraction in everyday explanation. *Psychonomic Bulletin & Review*, 24, 1451-1464. doi:10.3758/s13423-017-1299-3#ref-CR13

Berg, W., & Johnson, R. (1979). Assessing the impact of Victimization: Acquisition of the victim role among elderly and female victims. In W. Parsonage (Ed.), *Perspectives on victimology*. Beverly Hills, California: Sage.

- Berger, J., & Milkman, K. L. (2012). What Makes Online Content Viral? *Journal of Marketing Research*, 49(2), 192-205. doi:10.1509/jmr.10.0353
- Brundage, L. E., Derlega, V. J., & Cash, T. F. (1976). The Effects of Physical Attractiveness and Need for Approval on Self-Disclosure. *Personality and Social Psychology Bulletin*, 3(1), 63-66. doi:10.1177/014616727600300108
- Canadian Centre for Child Protection. (n.d.). *Sextortion*. Retrieved from Cybertip.ca: Canada's National Tipline For Reporting The Online Sexual Exploitation Of Children: https://www.cybertip.ca/app/en/internet_safety-sexortion
- Carlton, A. (2020). Sextortion: The Hybrid "Cyber-Sex" Crime. *North Carolina Journal of Law & Technology*, 21(3), 177-215.
- Chen, Q. (2017, August 2). *Time for ASEAN to Get Serious About Cyber Crime: ASEAN should look to forge its own cyber agreement*. Retrieved from The Diplomat: <https://thediplomat.com/2017/08/time-for-asean-to-get-serious-about-cyber-crime/>
- Choi, K.-S. (2008). Computer Crime Victimization and Integrated Theory: An Empirical Assessment. *International Journal of Cyber Criminology*, 2(1), 308-333.
- Citron, D. K., & Franks, M. A. (2014). Criminalizing Revenge Porn. *Wake Forest Law Review*, 49, 345-391.
- Clarke, R. V., & Cornish, D. B. (1985). Modeling Offenders' Decisions: A Framework for Research and Policy. *Crime and Justice*, 6, 147-185.
- CNA (Director). (2019). *The Dark Web: Ep1: Queen of Sextortion* [Motion Picture].
- Cohen, L. E., & Felson, M. (1979). Social Change and Crime Rate Trends: A Routine Activity Approach. *American Sociological Review*, 44(4), 588-608. doi:10.2307/2094589
- Council of Europe. (n.d.). *Convention on Cybercrime*. Retrieved from Council of Europe: <https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/185>
- Das, E., de Wit, J., & Stroebe, W. (2003). Fear Appeals Motivate Acceptance of Action Recommendations: Evidence for a Positive Bias in the Processing of Persuasive Messages. *Personality and Social Psychology Bulletin*, 29(5), 650-654. doi:10.1177/0146167203029005009
- Davis, P. K. (2014). Toward Theory for Dissuasion (or Deterrence) by Denial: Using Simple Cognitive Models of the Adversary to Inform Strategy. *Deterrence by Denial: Theory, Practice, and Empiricism* (pp. 1-21). RAND Corporation.
- De Hoog, N., Stroebe, W., & De Wit, J. B. (2005). The impact of fear appeals on processing and acceptance of action recommendations. *Personality and Social Psychology Bulletin*, 31(1), 24-33. doi:10.1177/0146167204271321
- De Hoog, N., Stroebe, W., & De Wit, J. B. (2008). The processing of fear-arousing communications: How biased processing leads to persuasion. *Social Influence*, 3(2), 84-113. doi:10.1080/15534510802185836
- Demetriou, C., & Silke, A. (2003). A Criminological Internet 'Sting'. Experimental Evidence of Illegal and Deviant Visits to a Website Trap. *British Journal of Criminology*, 43(1), 213-222. doi:10.1093/bjc/43.1.213
- Dion, K., Berscheids, E., & Walster, E. (1972). What is Beautiful is Good. *Journal of Personality and Social Psychology*, 24(3), 285-290. doi:10.1.1.521.9955
- Ditto, P. H., Pizarro, D. A., Epstein, E. B., Jacobson, J. A., & Macdonald, T. K. (2006). Visceral Influences on Risk-Taking Behavior. *Journal of Behavioral Decision Making*, 19, 99-113. doi:10.1002/bdm.520
- Dopson, E. (2021, March 5). *Videos vs. Images: Which Drives More Engagement in Facebook Ads?* Retrieved from databox: <https://databox.com/videos-vs-images-in-facebook-ads>
- Eke, A. W., Maaik Helmus, L., & Seto, M. C. (2019). A Validation Study of the Child Pornography Offender Risk Tool (CPORT). *Sexual Abuse*, 31(4), 456-476. doi:10.1177/1079063218762434
- EUROPOL. (2017). *Online Sexual Coercion and Extortion As A Form of Crime Affecting Children: Law Enforcement Perspective*. European Union Agency for Law Enforcement Cooperation.

- FBI's Internet Crime Complaint Center. (2016). *2016 Internet Crime Report*. Retrieved from https://pdf.ic3.gov/2016_IC3Report.pdf
- Felson, M. (1995). Those who discourage crime. In J. E. Eck, & D. Weisburd (Eds.), *Crime and Place (Crime Prevention Studies)* (Vol. 4, pp. 53-66). Criminal Justice Press.
- Felson, M. (2003). The Process of Co-offending. In *Crime Prevention Studies* (Vol. 16, pp. 149-167).
- Felson, M. (2009). The natural history of extended co-offending. *Trends in Organized Crime*, 12, 159-165. doi:10.1007/s12117-008-9056-7
- Flynn, E. (2015, January 21). *Vice*. Retrieved from Someone's Been Using My Facebook Photos to 'Catfish' People for Nearly a Decade: <https://www.vice.com/en/article/mv5zbn/someones-been-using-my-identity-to-catfish-people-for-nearly-ten-years-930>
- Furrow, J. L., King, P. E., & White, K. (2004). Religion and Positive Youth Development: Identity, Meaning, and Prosocial Concerns. *Applied Developmental Science*, 8(1), 17-26. doi:10.1207/S1532480XADS0801_3
- Gercke, M. (2006). The Slow Wake of A Global Approach Against Cybercrime. *Computer Law Review International*, 7(5), 140-145. doi:10.9785/ovs-cri-2006-140
- Gercke, M. (2014, November). *Understanding cybercrime: phenomena, challenges and legal response*. Retrieved from ITU: https://www.itu.int/en/ITU-D/Cybersecurity/Documents/Cybercrime2014_E.pdf
- Goldman, Z. K., & McCoy, D. (2016). Deterring Financially Motivated Cybercrime. *Journal of National Security Law & Policy*, 8(3), 595-619.
- Gordon, G. R., Curtis, G. E., & Willox, N. A. (2000). *The Growing Global Threat of Economic and Cyber Crime*. The National Fraud Center, Inc.
- Hardy, S. A., Walker, L. J., Rackham, D. D., & Olsen, J. A. (2012). Religiosity and Adolescent Empathy and Aggression: The Mediating Role of Moral Identity. *Psychology of Religion and Spirituality*, 4(3), 237-248. doi:10.1037/a0027566
- Harris, A. (2013, January 18). *Slate*. Retrieved from Who Coined the Term "Catfish"?: <https://slate.com/culture/2013/01/catfish-meaning-and-definition-term-for-online-hoaxes-has-a-surprisingly-long-history.html>
- Heiman, J. R. (1980). Female Sexual Response Patterns: Interactions of Physiological, Affective, and Contextual Cues. *Arch Gen Psychiatry*, 37, 1311-1316. doi:10.1001/archpsyc.1980.01780240109013
- Henson, B. (2020). Routine Activities. In Thomas J. Holt, & Adam M. Bossler (Eds.), *The Palgrave Handbook of International Cybercrime and Cyberdeviance* (pp. 469-487). Switzerland: Palgrave Macmillan. doi:10.1007/978-3-319-78440-3_23
- Heo, S. (2021, May 11). *Social media in South-east Asia: skeptical Singaporeans rank first*. Retrieved from The Business Times: <https://www.businesstimes.com.sg/asean-business/social-media-in-south-east-asia-skeptical-singaporeans-rank-first>
- Hindelang, M. J., Gottfredson, M. R., & Garofalo, J. (1978). *Victims of Personal Crime: An Empirical Foundation for a Theory of Personal Victimization*. Cambridge, MA: Ballinger Publishing Company.
- Holt, T. J., & Bossler, A. M. (2008). Examining the Applicability of Lifestyle-Routine Activities Theory for Cybercrime Victimization. *Deviant Behavior*, 30(1), 1-25. doi:10.1080/01639620701876577
- Hong, S., Lu, N., Wu, D., Jimenez, D. E., & Milanaik, R. L. (2020). Digital sextortion : Internet predators and pediatric interventions. *Current Opinion in Pediatrics*, 32(1), 192-197. doi:10.1097/MOP.0000000000000854
- Ibrahimi, S., Dervishi, E., & Ibrahimi, E. (2018). Cyberdeviance and the Role of Data Privacy Officer's Sustainable Structures in its Prevention. *Open Journal for Psychological Research*, 2(2), 61-68. doi:10.32591/coas.ojpr.0202.020611
- Ireland, C. A., Alderson, K., & Ireland, J. L. (2015). Sexual Exploitation in Children: Nature, Prevalence, and Distinguishing Characteristics Reported in Young Adulthood. *Journal of Aggression, Maltreatment & Trauma*, 24, 603-622. doi:10.1080/10926771.2015.1049765

- Jacobs, H., & Franks, M. A. (n.d.). *Cyber Civil Rights Initiative*. Retrieved from Definitions: <https://www.cybercivilrights.org/definitions/>
- Jaishankar, K. (2008). Space Transition Theory of Cyber Crimes. In Frank Schmalleger, & Michael Pittaro (Eds.), *Crimes of the Internet* (pp. 283-301). Upper Saddle River, NJ: Prentice Hall.
- Johnston, M. E., Sherman, A., & Grusec, J. E. (2013). Predicting moral outrage and religiosity with an implicit measure of moral identity. *Journal of Research in Personality, 47*(3), 209-217. doi:10.1016/j.jrp.2013.01.006
- Julien, E., & Over, R. (1988). Male sexual arousal across five modes of erotic stimulation. *Archives of Sexual Behavior, 17*(2), 131-143. doi:10.1007/BF01542663
- Jurecic, Q., Spera, C., Wittes, B., & Poplin, C. (2016, May 11). *Sextortion: The problem and solutions*. Retrieved from Brookings: <https://www.brookings.edu/blog/techtank/2016/05/11/sextortion-the-problem-and-solutions/>
- Kemp, S. (2021, February 9). *Digital 2021: Singapore*. Retrieved from Datareportal: <https://datareportal.com/reports/digital-2021-singapore>
- Kidd, R. F., & Chayet, E. F. (1984). Why Do Victims Fail to Report? The Psychology of Criminal Victimization. *Journal of Social Issues, 40*(1), 39-50.
- Kitcher, P. (1981). Explanatory Unification. *Philosophy of Science, 48*(4), 507-531.
- Knight, R. A., & Prentky, R. A. (1990). Classifying Sexual Offenders: The development and corroboration of taxonomic models. In W. L. Marshall, D. R. Laws, & H. E. Barbaree, *Applied clinical psychology. Handbook of sexual assault: Issues, theories, and treatment of the offender* (pp. 23-52). Plenum Press.
- Koh, T. (2021). *Social Media Marketing Singapore: The Complete Guide*. Retrieved from MediaOne: https://mediaonemarketing.com.sg/social-media-marketing-singapore-guide/#Statistics_About_Social_Media_Usage_in_Singapore
- Kopecký, K. (2017). Online blackmail of Czech children focused on so-called "sextortion" (analysis of culprit and victim behaviors). *Telematics and Informatics, 34*(1), 11-19. doi:10.1016/j.tele.2016.04.004
- Kopecký, K., Hejsek, L., Kusá, J., & Řeřichová, V. (2015). Specifics of children communication and online aggressors within the online assaults on children (analysis of selected utterances). *SGEM International Multidisciplinary Scientific Conferences on Social Sciences and Arts*. Albena, Bulgaria.
- Kusumasondjaja, S. (2018). The roles of message appeals and orientation on social media brand communication effectiveness: An evidence from Indonesia. *Asia Pacific Journal of Marketing and Logistics, 30*(4), 1135-1158. doi:10.1108/APJML-10-2017-0267
- Lanning, K. V. (2010). *Child Molesters: A Behavioral Analysis for Professionals Investigating the Sexual Exploitation of Children*. National Center for Missing & Exploited Children.
- Lea, S. E., Fischer, P., & Evans, K. M. (2009). *The psychology of scams: Provoking and committing errors of judgement*. Office of Fair Trading.
- Liggett, R. (2019). Exploring online sextortion offenses: Ruses, demands, and motivations. *Sexual Assault Report, 22*(4), 58-62.
- Long, A. (2015). Deterrence: The State of the Field. *International Law and Politics, 47*, 374-376.
- Lorenzo-Dus, N., & Izura, C. (8th September 2016, September 8). The truth about online grooming. *British Science Festival*. Swansea University .
- Lorenzo-Dus, N., Izura, C., & Pérez-Tattam, R. (2016). Understanding grooming discourse in computer-mediated environments. *Discourse, Context and Media, 12*, 40-50. doi:10.1016/j.dcm.2016.02.004
- McGlynn, C., Rackley, E., & Houghton, R. (2017). Beyond 'Revenge Porn': The Continuum of Image-Based Sexual Abuse. *Feminist Legal Studies, 25*, 25-46. doi:10.1007/s10691-017-9343-2

- McKeever, N. (2020). Why, and to What Extent, Is Sexual Infidelity Wrong? *Pacific Philosophical Quarterly*, 101(3), 515-537. doi:10.1111/papq.12316
- McKenna, K. Y., & Bargh, J. A. (1999). Causes and Consequences of Social Interaction on the Internet: A Conceptual Framework. *Media Psychology*, 1(3), 249-269. doi:10.1207/s1532785xmep0103_4
- Ministry of Home Affairs. (2016, July 20). *National Cybercrime Action Plan*. Retrieved from Ministry of Home Affairs: <https://www.mha.gov.sg/docs/default-source/press-releases/ncap-document.pdf>
- Modarres, M., Mandelcorn, S., & Mosleh, A. (2013). An Explanatory Model of Cyber-Attacks Drawn from Rational Choice Theory. *American Nuclear Society Meeting on Risk Management for Complex Socio-Technical Systems (RM4CSS)*. Washington, DC: Transactions of the American Nuclear Society.
- National Crime Agency. (2018). *Record numbers of UK men fall victim to sextortion gangs*. Retrieved from National Crime Agency: <https://www.nationalcrimeagency.gov.uk/news/record-numbers-of-uk-men-fall-victim-to-sextortion-gangs>
- Norman, D. A. (2002). Emotion & Design: Attractive Things Work Better. *Interactions*, 9(4), 36-42. doi:10.1145/543434.543435
- O'Malley, R. L., & Holt, K. M. (2020). Cyber Sextortion: An Exploratory Analysis of Different Perpetrators Engaging in a Similar Crime. *Journal of Interpersonal Violence*, 0(0), 1-26. doi:10.1177/0886260520909186
- O'Neill, S., Mawry, R. e., & Adamson, D. S. (2016, October 26). *The Skype sex scam - a fortune built on shame*. Retrieved from BBC News: <https://www.bbc.com/news/magazine-37735369>
- Parry, S. (2017, February 10). *South China Morning Post*. Retrieved from Sextortion, lies and videotape: the Philippine cybercriminals who target men in Hong Kong and worldwide : <https://www.scmp.com/magazines/post-magazine/long-reads/article/2069492/sextortion-lies-and-videotape-philippine>
- Pass, J. A., Siegwart, L., & Park, J. H. (2009). All you need is love: Is the sociometer especially sensitive to one's mating capacity? *European Journal of Social Psychology*, 40(2), 221-234. doi:10.1002/ejsp.619
- Patchin, J. W., & Hinduja, S. (2018). Sextortion Among Adolescents: Results From a National Survey of U.S. Youth. *Annals of Sex Research*, 32(1), 30-54. doi:10.1177/1079063218800469
- Patchin, J. W., & Hinduja, S. (2020). Sextortion Among Adolescents: Results From a National Survey of U.S. Youth. *Sexual Abuse*, 32(1), 30-54. doi:10.1177/1079063218800469
- Paul, K. (2019, August 23). *Market Watch*. Retrieved from 'I was humiliated' — online dating scammers hold nude photos for ransom in 'sextortion': <https://www.marketwatch.com/story/i-was-humiliated-online-dating-scammers-hold-nude-photos-for-ransom-in-sextortion-attacks-2019-03-06>
- Perina, A. (2015). Black Holes and Open Secrets: The Impact of Covert Action on International Law. *Columbia Journal of Transnational Law*, 53(3), 507-583.
- Phoebe. (2017, March 26). *ASEAN Today*. Retrieved from Chinese love scams: Preying on Singapore's most vulnerable people: <https://www.aseantoday.com/2017/03/chinese-love-scams-preying-on-singapores-most-vulnerable-people/>
- Piquero, A. R., & Hickman, M. (2002). The Rational Choice Implications of Control Balance Theory. In A. R. Piquero, & S. G. Tibbets (Eds.), *Rational Choice and Criminal Behavior* (1st ed.). Routledge.
- Powell, A., Henry, N., Flynn, A., & Scott, A. J. (2019). Image-based sexual abuse: The extent, nature, and predictors of perpetration in a community sample of Australian residents. *Computers in Human Behavior*, 92, 393-402. doi:10.1016/j.chb.2018.11.009
- Powell, D. (2021, March 16). *What to Do If You Are the Victim of Facebook Sextortion*. Retrieved from Minc Law: <https://www.minclaw.com/facebook-sextortion-help/>
- Reyns, B. W., Henson, B., & Fisher, B. S. (2011). Being Pursued Online: Applying Cyberlifestyle–Routine Activities Theory to Cyberstalking Victimization. *Criminal Justice and Behavior*, 38(11), 1149-1169. doi:10.1177/0093854811421448

Ryan, J. (2018, August 10). *The Sun*. Retrieved from Sextortion: Who are really behind those Facebook invitations from beautiful girls you don't know? Meet the con artists tricking men into sending sex photos before blackmailing them for thousands of pounds: <https://www.thesun.co.uk/news/6978369/facebook-scammers-posing-as-beautiful-women-are-conning-men-into-sending-sex-photos-before-blackmailing-them-for-thousands-of-pounds/>

Sedikides, C., & Gebauer, J. E. (2009). Religiosity as Self-Enhancement: A Meta-Analysis of the Relation Between Socially Desirable Responding and Religiosity. *Personality and Social Psychology Review*, 14(1), 17-36. doi:10.1177/1088868309351002

Seto, M. C., & Eke, A. W. (2015). Predicting recidivism among adult male child pornography offenders: Development of the Child Pornography Offender Risk Tool (CPORT). *Law and Human Behavior*, 39(4), 416-429. doi:10.1037/lhb0000128

Seto, M. C., & Eke, A. W. (2017). Correlates of admitted sexual interest in children among individuals convicted of child pornography offenses. *Law and Human Behavior*, 41(3), 305-313. doi:10.1037/lhb0000240

Shinners, E., & Morgan, B. L. (2009). Effects of The "What is Beautiful is Good" Stereotype on Perceived Trustworthiness. *UW-L Journal of Undergraduate Research XII*.

Singapore Business Review. (2020, July 2). *Singaporeans reveal utmost concern over data security*. Retrieved from Singapore Business Review: <https://sbr.com.sg/information-technology/news/singaporeans-reveal-utmost-concern-over-data-security>

Singapore Economic Development Board. (2021, April 9). *EDB Singapore*. Retrieved from <https://www.edb.gov.sg/en/why-singapore/an-economic-powerhouse.html>

Singapore Police Force. (2020, June 22). *Singapore Police Force*. Retrieved from Police Advisory On Cyber Extortion: https://www.police.gov.sg/media-room/news/20200622_others_police_advisory_on_cyber_extortion_scams

Sinnamon, G. (2017). The Psychology of Adult Sexual Grooming: Sinnamon's Seven-Stage Model of Adult Sexual Grooming. In W. Petherick, & G. Sinnamon (Eds.), *The Psychology of Criminal and Antisocial Behavior: Victim and Offender Perspectives* (pp. 459-487). Academic Press.

Skakoon-Sparling, S., Cramer, K. M., & Shuper, P. A. (2016). The Impact of Sexual Arousal on Sexual Risk-Taking and Decision-Making in Men and Women. *Archives of Sexual Behavior*, 45, 33-42. doi:10.1007/s10508-015-0589-y

Stebbins, A. (2021, March 12). *Minc*. Retrieved from Do Sextortionists Follow Through on Their Threats to Release Embarrassing Images & Videos?: <https://www.minclaw.com/do-sextortionists-follow-through/>

Suler, J. (2004). The online disinhibition effect. *CyberPsychology & Behavior*, 7(3), 321-326. doi:10.1089/1094931041291295

Tafasse, W., & Wlen, A. (2018). Using message strategy to drive consumer behavioral engagement on social media. *Journal of Consumer Marketing*, 35(3), 241-253. doi:10.1108/JCM-08-2016-1905

Tewksbury, R. A., & Mustaine, E. E. (2010). Cohen, Lawrence E., and Marcus K. Felson: Routine Activity Theory. In F. T. Cullen, & P. Wilcox (Eds.), *Encyclopedia of Criminological Theory* (pp. 187-193). SAGE Publications. doi:10.4135/9781412959193.n52

Today. (2021, February 10). *Today*. Retrieved from Crimes reported in S'pore rose 6.5% in 2020, fuelled by 65% jump in scam cases with over S\$200m lost: <https://www.todayonline.com/singapore/crimes-reported-spore-rose-65-2020-fuelled-65-jump-scam-cases-over-s200m-lost>

Uhrig, M. K., Trautmann, N., Baumgärtner, U., Treede, R.-D., Henrich, F., Hiller, W., & Marschall, S. (2016). Emotion Elicitation: A Comparison of Pictures and Films. *Frontiers in Psychology*, 7(180). doi:10.3389/fpsyg.2016.00180

UNODC. (2013, February). *Comprehensive Study on Cybercrime*. Retrieved from United Nations Office on Drugs and Crime: https://www.unodc.org/documents/organized-crime/UNODC_CCPCJ_EG.4_2013/CYBERCRIME_STUDY_210213.pdf

UNODC. (2019, February). *Harmonization of laws*. Retrieved from United Nations Office on Drugs and Crime: <https://www.unodc.org/e4j/en/cybercrime/module-3/key-issues/harmonization-of-laws.html>

- UNODC. (2020, September 22). *United Nations Office on Drugs and Crime*. Retrieved from Preventing sextortion: a new Internet crime on the rise during COVID-19: <https://www.unodc.org/westandcentralafrica/en/2020-09-22-sextortion-cyber-crime.html>
- Van Hooff, J. (2017). An everyday affair: deciphering the sociological significance of women's attitudes towards infidelity. *The Sociological Review*, 65(4), 850-864. doi:10.1111/1467-954X.12417
- Vitell, S. J., Bing, M. N., Davison, H., Ammeter, A. P., Garner, B. L., & Novicevic, M. M. (2009). Religiosity and Moral Identity: The Mediating Role of Self-Control. *Journal of Business Ethics*, 88(4), 601-613. doi:10.1007/s10551-008-9980-0
- Ward, S. J., & King, L. A. (2018). Moral Self-Regulation, Moral Identity, and Religiosity. *Journal of Personality and Social Psychology*, 115(3), 495-525. doi:10.1037/pspp0000207
- Whitworth, D. (2018, May 24). *Sextortion: Big rise in victims with 'tens of thousands at risk'*. Retrieved from BBC News: <https://www.bbc.com/news/newsbeat-43433015>
- Wittes, B. (2017). Cyber Extortion and International Justice. *Georgetown Journal of International Law*, 48(3), 941+.
- Wolak, J., & Finkelhor, D. (2016, June). *Sextortion: Findings from a Survey of 1631 Victims*. Retrieved from https://humantraffickingsearch.org/wp-content/uploads/2018/09/Sextortion_Report.pdf
- Wolak, J., Finkelhor, D., Walsh, W., & Treitman, L. (2018). Sextortion of Minors: Characteristics and Dynamics. *Journal of Adolescent Health*, 62(1), 72-79. doi:10.1016/j.jadohealth.2017.08.014
- Wolff, J. (2018, February 12). *The Real Reasons Why Cybercrimes May Be Vastly Undercounted*. Retrieved from Slate: <https://slate.com/technology/2018/02/the-real-reasons-why-cybercrimes-are-vastly-underreported.html>
- World Economic Forum. (2015). *The Human Capital Report 2015*. World Economic Forum.
- Wright, C. S. (2010). Criminal Specialization as a corollary of Rational Choice. SSRN. doi:10.2139/ssrn.3461064
- Yu, L., Guan, Z., & Ramaswamy, S. (2016). The effect of time zone difference on asynchronous communications in global software development. *International Journal of Computer Applications in Technology*, 53(3), 213-225. doi:10.1504/IJCAT.2016.075523
- Yuen, M. (2020, April 23). *Online 'sextortion' cases spike*. Retrieved from TheStar: <https://www.thestar.com.my/news/nation/2020/04/23/online-sextortion-cases-spike>
- Zamarian, L., Weiss, E. M., & Delazer, M. (2011). The Impact of Mild Cognitive Impairment on Decision Making in Two Gambling Tasks. *The Journals of Gerontology*, 66B(1), 23-31. doi:10.1093/geronb/gbq067
- Zhao, N., Zhou, M., Yuanyuan, S., & Jianxin, Z. (2015). Face Attractiveness in Building Trust: Evidence From Measurement of Implicit and Explicit Responses. *Social Behavior and Personality*, 43(5), 855-866. doi:10.2224/sbp.2015.43.5.855
- Zhuang, Q., Wang, L., Tang, Y., & Chen, A. (2016). Translation of fear reflex into impaired cognitive function mediated by worry. *Science Bulletin*, 61(24), 1841-1843. doi:10.1007/s11434-016-1177-9

TERRORISM

TOWARDS A YOUTH-CENTRIC APPROACH IN THE REHABILITATION OF RADICALISED YOUTHS

Ng Li Ling
Ministry of Home Affairs, Singapore

ABSTRACT

The uptick of self-radicalised adolescents is a growing concern worldwide. Singapore has seen a similar upward trend, and the radicalised youth cases are getting younger. This is largely precipitated by the presence of various radicalising influences across the cyberspace, including targeted virulent propaganda by the Islamic State in Iraq and Syria (ISIS), which continues to appeal to the vulnerable and misguided. In concert with the critical developmental stage and prevailing socio-technological environment of these radicalised youths, research has indicated the presence of distinct psychosocial needs and vulnerabilities that should be considered in tailoring rehabilitation interventions for such youths. These findings have encouraged a shift in Singapore's terrorist rehabilitation programme from the traditional radicalisation-specific risk-reduction approach to the adoption of a developmentally-informed approach, taking into account the youths' life stage and potential for positive change in facilitating their transition towards a non-extremist life trajectory. This article explores initiatives at various ecological levels (e.g. family, community etc.) anchoring Singapore's rehabilitation programmes for radicalised youths, and the importance of upstream efforts in preventing radical ideology from taking root in Singapore's context.

TRENDS IN YOUTH RADICALISATION

The phenomenon of radicalisation among youths has become an emergent security threat globally (Barracosa & March, 2022; Cherney et al., 2020; Siegel et al., 2019). Notwithstanding youths' historic presence in the extremism context (i.e. active participation in liberation and resistance movements etc.), experts have been pointing out that they now form a disproportionate representation within the violent extremist population (Barracosa & March, 2022). They are also reported to be increasingly implicated at progressively younger ages (Campelo et al., 2018; Siegel et al., 2019). In the absence of a universally agreed definition in literature, this article adopts a working definition of the term "radicalisation" as the process of adopting an "extremist belief system", including the "willingness to condone, support, facilitate or use violence to further political, ideological, religious or other goals"

(Human Rights Council, 2016; Siegel et al., 2019). Youths are defined here as those under the age of 21 years old.

At the international level, a stark increase in the number of "homegrown terrorists" (i.e. born and bred in their respective countries) subscribing to violent radical Islamist ideologies has been keenly observed with the rise of the Islamic State in Iraq and Syria (ISIS) in mid-2014 (Campelo et al., 2018). In Singapore, this trend is similarly reflected in the uptick in self-radicalised cases detected since 2015 and found to have adopted radical ideologies via "self-learning and without a pre-existing physical affiliation with a terrorist group" (Robert, 2018).

Specifically, from 2015 to September 2022, eight of the 33 self-radicalised Singaporeans dealt with under the Internal Security Act (ISA) were aged between 16 and 20 (Tuen, 2021). In comparison, the

youngest radicalised individual dealt with under the ISA prior to 2015 was 20 years old (Hariz, 2021a). This suggests that in tandem with the evolving terrorism landscape, youths are likely to possess vulnerabilities that render them more susceptible to radicalisation, specifically through self-radicalisation via online means, which presently serves as the primary driver of the domestic terrorism threat in Singapore's context (Internal Security Department; ISD, 2022b; Robert, 2018).

Despite its major territorial and leadership losses in the core conflict zone in Iraq and Syria, ISIS continues to pose a serious terrorism threat to Southeast Asia, including Singapore (Institute for Economics & Peace; IEP, 2022; ISD, 2022b). ISIS has been particularly effective in radicalising youths due to its targeted and concerted online propaganda efforts which experts describe as a robust "pro-ISIS eco-system" (ISD, 2022b). Such efforts prey on the youths' developmental specificities, easy internet access and continual exposure to related radicalising influences (Borum & Patterson, 2019; Heinke & Persson, 2016; T'ng, 2019). Hence, considering the prevailing porous socio-technological environment that youths are embedded within, they are also likely to be at risk from other forms of radicalising influences online, including precipitated spillover effects of external events and developments that may fuel social grievances and a desire for action (Adam-Troian, Tecmen & Kaya, 2021).

As a result, far-right extremism, which presently still predominates the Western scene (IEP, 2022b), have since broadened the scope of the terrorism threat in the region (ISD, 2021a). In December 2020, a 16-year-old Singaporean youth was detained under the ISA for planning to mount attacks against Muslims at two mosques in Singapore. He was the youngest detainee and the first Singaporean to be inspired by far-right extremist ideologies (ISD, 2021a). This case lends testimony to the growing threat posed by far-right extremism globally and how threat perceptions (e.g. affiliative, economic, and existential) in response to global and local events could propel youths towards violence as means of a compensatory response (Adam-Troian, Tecmen & Kaya, 2021; ISD, 2021a).

DEVELOPMENTAL SPECIFICITIES

Despite growing interest in youth radicalisation, studies across various key disciplines including psychology, criminology and political science, have yet to establish sufficient evidence of a distinct profile or single trajectory for youths (Campelo et al., 2018; Cherney et al., 2020). This is because the phenomenon remains complex and has been found to comprise a multiplicity of interacting risk factors across individual (psychological vulnerabilities), environmental (relational and proximal micro-environment), and societal (cultural and macro-environment) contexts (Campelo et al., 2018; Doosje et al., 2016; Rolling et al., 2022). Hence, existing research suggests there is value in adopting a developmental psychology perspective (Adam-Troian, Tecmen & Kaya, 2021; García-Coll & Marks, 2017; Schroder et al., 2022) and an ecological systemic model in understanding youth radicalisation, given similar niches that at-risk and antisocial youths have been conventionally found within (Campelo et al., 2018; Bersnak & Prezelj, 2020; Siegel et al., 2019). Present evidenced-based research, while in its infancy, has similarly outlined support for the need to consider developmental specificities and fragilities, such as biological and social-psychological vulnerabilities associated with adolescence, in informing tailored responses and interventions to prevent youth radicalisation (Bronsard, Cherney & Vermeulen, 2022; Heinke & Persson, 2016; Oppetit et al., 2019).

Adolescence, typically characterised as a period of identity development and formation (Erikson, 1968), has been found to be a specific risk factor distinguishing youths from older groups of radicalised individuals (Oppetit et al., 2019). During this phase of reorganisation, the detachment from one's primary care givers in search of one's own identity and autonomy can give rise to anxieties surrounding insecurity and abandonment (Rolling et al., 2022). This sense of personal uncertainty, also widely established as a key determinant of a radical belief system (Doosje, Loseman & Van Den Bos, 2013), thus renders adolescents susceptible to radical narratives and identification with a radical community or group (Campelo et al., 2018), which often serves as a means for them to achieve a sense of belonging and personal significance (Kruglanski et al., 2013). The structured and

dichotomous worldview that such community or group provides also engenders a greater sense of perceived clarity and comfort among youths (Dhami & Murray, 2016; Doosje et al., 2016). Furthermore, it is not uncommon for radicalised youths to present with an idealistic dimension (Van San, Sieckelincx & de Winter, 2013) in their quest for identity, where they may seek to glorify their commitment towards the identified cause or group, as a compensatory means to further reduce the uncertainty experienced (Hogg, 2007; Hogg, Meehan & Farquharson, 2010).

In addition, considerable research has found that adolescents tend to have a reduced ability to regulate their emotional responses and an increased threat sensitivity (Slivers et al., 2012; Steinberg, 2008). Developmental changes in the brain's dopaminergic system responsible for social information and reward processing takes place during puberty (Blakemore, 2018; Steinberg, 2008). Compared to adults, adolescents are more likely to demonstrate a higher proclivity for sensation seeking and risk taking, and lowered capacities for self-regulation and consequential thinking (Martin et al., 2002). Furthermore, they are also likely to possess fewer "guidelines" and lived experiences that can be important in inculcating life lessons, as well as normative and value systems (e.g. ethical and political awareness, personal resilience) to help navigate difficulties effectively (Hariz, 2021a; Schroder et al., 2022). This includes an absence of anchors in life (e.g. familial and work commitments) that can potentially balance and broaden their life perspectives. Within the context of radicalisation, youths, particularly those experiencing identity conflicts, are hence prone to engaging in negative and extreme responses towards diverse environmental stressors, including the pursuit of violent extremist causes (Campelo et al., 2018; Oppetit et al., 2019; Ventriglio & Bhugra, 2019).

Such findings suggest that adolescence is not only representative of an age span but instead a critical developmental life stage where various cognitive, motivational, social, and practical competencies (e.g. education, gender identity, relational skills etc.) are attained (Pels & de Ruyter, 2012; Schroder et al., 2022). Similarly, the process of acquiring these competencies is not without influence by peers, family and society (Borum,

2011; Campelo et al., 2022). This indicates the importance for rehabilitation to provide a structured and supportive environment that allows radicalised youths to develop a stable alternative identity, alongside the relevant developmental competencies to be acquired during this period (Barracosa & March, 2022; Zych & Nasaecru, 2021).

SHIFTS TOWARDS YOUTH-CENTRICITY

Singapore's terrorist rehabilitation programme was formulated in the early 2000s, in the aftermath of a series of arrests involving members of the homegrown cell of Jemaah Islamiyah (JI), a regional Islamist militant group which aimed to create a *Daulah Islamiyah* (Islamic state) in the region through the use of violence (ISD, 2021b). The programme, involving close partnerships between the authorities and community partners, such as the Religious Rehabilitation Group (RRG) – a volunteer group of Islamic scholars and teachers – and Inter-Agency Aftercare Group (ACG), an informal network of Muslim organisations, relies on a holistic, comprehensive, and long-term strategy comprising religious, psychological and social interventions to promote rehabilitation (Koh, 2021b; ISD, 2021b). The three-pronged multidisciplinary strategy is customised towards the needs of each radicalised individual, to address their propensity for hatred and violence, as well as vulnerability to radical influences, to maximise their chances of successful rehabilitation and reintegration into society (Koh, 2021b; Tuen, 2021).

Addressing radical ideological misconceptions that underpin radical mind-sets remains at the forefront of rehabilitation given its significance in the radicalisation process. However, the uptrend of younger self-radicalised cases presenting with a multitude of non-ideological issues (e.g., sense of belonging and identity, lack of critical thinking skills to discern radical rhetoric and mental resilience to cope with stressors etc.) points to a need to consider idiosyncratic youth-related factors across different ecological circles in relation to one's radicalisation process (Hariz, 2021a; Robert, 2018; Tuen, 2021). Thus, Singapore has since refined its terrorist rehabilitation programme to incorporate a more developmentally-informed and integrated approach over the years. This includes additional attention paid to non-ideological

factors as well as psychosocial vulnerabilities tied with adolescence, including the associated mental, intellectual, and emotional maturities or capacities of the radicalised youth (Hariz, 2021a; Koh, 2021a).

Complementary Strengths-based Approaches to Rehabilitation

Strength-based approaches to complement rehabilitation tap on the inherent positive potential of youths by maximising their strengths and capabilities, in areas of education, mental, physical, emotional, and social development, to successfully reintegrate them into society (Bronsard et al., 2022; Lefas & Nozawa, 2016; Robert, 2018). This is because youth identification with radical ideas or influences appears closely tied to adolescence-specific factors, and are found receptive to de-radicalisation programmes once relevant developmental competencies are acquired and identity issues are addressed (Bronsard et al., 2022; Ventriglio & Bhugra, 2019). Alongside radicalisation-specific factors, psychological rehabilitation thus focuses on exploring the youths' aspirations and goals, with the aim of cultivating prosocial values and prioritising adaptive pursuits relative to one's ideological commitment. Efforts are placed at amplifying protective factors of the youths by empowering and equipping them with the necessary capabilities to meet their needs via more adaptive and prosocial means. Youth-specific standardised psychometric and clinical assessments are also utilised to acquire a more accurate and effective understanding of the youths' functioning in various domains (e.g. cognitive, emotional etc.) to inform case formulation and management plans (Barracosa & March, 2022; Robert, 2018).

Apart from incorporating approaches that target non-ideological risk factors as well as protective factors into Singapore's terrorist rehabilitation programme, a mentorship programme was also introduced in 2016 to help youths better navigate important issues (e.g., identity issues, goal-setting, etc.) related to adolescence and adulthood (Tuen, 2021). A mentor functions as a positive influence for youths and provides them with additional social support to mitigate their risk of re-engagement in terrorism-related activities post-release (Hafiz,

2021b; Koh, 2021b). Mentors have the added benefit of likely being perceived as neutral interlocutors unaffiliated with the authorities and as credible adults whom the youths may trust and rely on for help and support (Lefas & Nozawa, 2016; Siegel et al., 2019). Mentors have been provided with upskilling opportunities in the form of relevant workshops in the context of extremism, such as a CENS (Centre of Excellence for National Security) Workshop on Life Psychological Intervention organised by the S. Rajaratnam School of International Studies (RSIS) of Nanyang Technological University in 2018 (RSIS, 2018). In the workshop, mentors were coached on mentoring tools based on Denmark's Aarhus model of anti-radicalisation to aid mentees in developing the necessary general life skillset and mind-set to deal with current and future life challenges while steering clear of terrorism-related activities (Anonymous, 2019; Bertelsen, 2015).

To illustrate, a self-radicalised Singaporean youth was assigned a mentor, who is a member of the RRG Secretariat and a Ministry of Education (MOE)-trained teacher, while in detention. Besides helping the youth with his schoolwork, the mentor also taught him various learning concepts, social interaction skills and coping strategies. Through the mentor's help, the youth performed well enough in the GCE 'O' Level examinations while in detention to qualify for admission to a polytechnic. The mentor-mentee relationship was also maintained after the youth's release from detention. The youth has been appreciative of the mentorship and rated the quality of his interactions with the mentor as a "9 out of 10".

Expansive Ecological Perspective in Addressing Youth Radicalisation

In adapting Singapore's terrorist rehabilitation programme towards dealing with radicalised youths, risk factors present at the micro-environmental context that contributed to the youth's radicalisation process are managed closely, apart from mitigating individual or person-related risk factors. This is because an enabling and supportive environment can help youths to develop useful associations with positive role models, dissociate themselves from antisocial or radical groups, and forge stronger familial ties (Siegel et al., 2019; Zych & Nasaescu, 2021). Schools in particular are important stakeholders,

given the significant amount of time youths spend in education, as well as their role in shaping youths' attitudes (e.g. perspective taking, social cohesion, respect towards others) and fostering prosocial identities (Robert, 2018; Siegel et al., 2019). In Singapore, local authorities work closely with families, schools and other stakeholders to make arrangements for youth detainees to continue receiving education where practicable, for example, by engaging tutors to guide them in specific academic subjects to prepare for national-level examinations (ISD, 2021b). This is intended to facilitate the youths' reintegration into mainstream society upon their release, whereupon they are also encouraged to engage in further educational pursuits or to seek gainful employment – which serve as protective factors that increase their stability and chances of successful reintegration into society (ISD, 2021b; Tuen, 2021; Siegel et al., 2019).

A 17-year-old-youth, "Daniel" (not his real name), who was detained in January 2020 for his support for ISIS, went from barely passing his Secondary 3 education (just prior to his arrest), to making tremendous improvements in his academic performance while in detention with the help of his tutors. He scored four distinctions out of five subjects in his GCE 'Normal' (Technical) level examinations in 2020 and passed all his subjects in his GCE 'Normal' (Academic) level examinations in 2021. His academic achievement was said to have a positive impact on his self-esteem and provided him with added motivation in his rehabilitation. "Daniel" also did well on the religious and psychological fronts – religious counselling sessions by the RRG counsellor helped to correct the misguided belief in radical ideologies which "Daniel" had imbibed from ISIS's violent propaganda, while the psychologist worked with "Daniel" to reduce his vulnerability to radical influences. Overall, "Daniel" made good progress in his rehabilitation and was released from detention in January 2022. He is currently furthering his education in a post-secondary institution while serving his Restriction Order (RO) (Hariz, 2021b; ISD, 2022a).

In youth radicalisation research, familial support has been identified as a key feature in determining an individual's resilience against radicalisation as well as integration potential upon release (Emmelkamp et al., 2020; Zych & Nasaescu, 2021; Radicalisation Awareness Network; RAN,

2017). In the Singapore programme, young detainees not only receive weekly family visits to ensure they receive sufficient social support, but the rehabilitation stakeholders such as the psychologists and aftercare officers also work closely with their families to strengthen the family system in promoting positive rehabilitation outcomes for them (Koh, 2021b). This includes coaching them on positive parenting practices (e.g. expression of disagreement towards radical ideas, improving communication styles), addressing potential undesirable influences and supporting their practical resource needs. Considering that the parents' ability to influence their children's sense of belonging and worldview is crucial for their moral and social development, an increasing focus is placed on working in tandem with the families of radicalised youths during earlier stages of their detention, to facilitate early intervention and a longer roadmap for change. There is also a shift towards adopting a family systems perspective, where family members are not only seen as providing a censoring and supportive environment for youths, but also active actors in their rehabilitation process.

This was observed in the case of "Daniel" above, where the involvement and support of his parents have been critical to the good progress he has made in his rehabilitation. Not only did they attend weekly visits without fail, their ability to view his detention positively, for example, as an opportunity for Daniel to focus on his studies and attain a more meaningful life outlook, have also been useful in shaping his own views and keeping him focused on his rehabilitation. Even during the Covid-19 'circuit breaker' period where family visits were suspended, Daniel's parents (alongside those of several other youth detainees) were encouraged to record video messages to show their continued support and maintain emotional connection to the youths (Hariz, 2021b; ISD, 2022a).

Embracing a Whole-Of-Community Approach

At a broader societal level, the wider community also plays a vital role in combatting the youth radicalisation threat (Siegel et al., 2019; RAN, 2017). On the rehabilitation front, stakeholders in Singapore carry out in-depth discussions and exercises with the radicalised youths on current affairs and relevant socio-religious issues. The goal

of these discussions is two-fold. Firstly, to inoculate the youths against radical influences that leverage on real world issues. Secondly, to help them to remain connected with their community, and in the process, better understand the context and manage the complexities when navigating their differing responsibilities in a secular and pluralistic country like Singapore. Such efforts have been observed to be useful at developing the critical thinking abilities of youths and shaping their intolerant political, ideological and religious positions beyond micro views of perceived injustice and discrimination towards a more holistic sociological perspective.

Moving upstream in the radicalisation continuum, community stakeholders are also best placed to contribute towards early intervention efforts to mitigate youths' vulnerabilities to radicalisation (Bersnak & Prezelj, 2020; Robert, 2018; Siegel et al., 2019). Such efforts can take the form of counter-ideology outreach initiatives aimed at strengthening youths' resilience against radical influences. In Singapore, the authorities have collaborated with community partners such as the RRG and ACG to conduct outreach efforts to various segments of the community including educators, students and youths to sensitise them to the threat of terrorism and the tell-tale indicators of radicalisation (RRG, 2016; Shanmugam, 2021). Through government-led initiatives such as the SGSecure movement, which aims to build vigilance, cohesion and resilience in the community, members of the public are also encouraged to report suspected cases of radicalisation promptly, so that early intervention can be made (Koh, 2021c; SGSecure, 2019).

In raising awareness of the importance of preventing youth radicalisation, youth-related outreach forums and events held in recent years have included the

online dialogue 'Raising Harmonious Youths' for youths and parents organised by the North Mosque Cluster in partnership with RRG and RSIS held in March 2021, and the workshop on Countering Violent Extremism (CVE) for Indian Muslim Youths by the South Mosque Cluster in collaboration with RRG and Ministry of Home Affairs (MHA) held in March 2022. Training workshops have also been conducted for local school counsellors and student welfare officers to equip them with the necessary skills and knowledge to identify and report potential student radicalisation cases (Koh, 2021c). These examples illustrate the intensified engagement efforts between governmental, families and communities at large to fortify social resilience against youth radicalisation.

CONCLUSION

The phenomenon of youth radicalisation remains a concern as youths have been found to present with developmental-specific vulnerabilities and needs that render them more susceptible to online radicalising influences compared to adults. Underlying themes of identity and uncertainty, expounded by their undeveloped cognitive and reward processing capacities, appear to be key youth-specific factors driving this phenomenon. Hence, as the profile of radicalised individuals shift towards a younger and more diverse demographic, there is a need for Singapore to continue to adapt and refine its rehabilitation approach to address the factors that contribute to their radicalisation. Specifically, it is important to continually build up youth-specific expertise and initiate cohesive efforts across the different ecological circles that youths are situated within (individual, environmental, societal), so as to bolster the provision of developmentally-informed support for radicalised youths in Singapore.

ABOUT THE AUTHOR

Ng Li Ling

is a psychologist with the Counter-Terrorism Research Division within the Ministry of Home Affairs, Singapore. She works with a team of psychologists undertaking psychological risk assessments, offering counselling services and managing the rehabilitation programmes for individuals detained for terrorism-related conduct and those under supervision regime, including self-radicalised individuals. The team also conducts psychological research of direct application to the field of counter-terrorism.

REFERENCES

- Adam-Troian, J., Tecmen, A., & Kaya, A. (2021). Youth extremism as a response to global threats? A threat-regulation perspective on violent extremism among the youth. *European Psychologist*, 26(1), 15–28. <https://doi.org/10.1027/1016-9040/a000415>
- Anonymous. (2019). Mentoring and Deradicalisation. In S. Jayakumar (Ed.), *Terrorism, Radicalisation & Countering Violent Extremism: Practical considerations & Concerns* (pp. 19–28). Springer Singapore.
- Barracosa, S., & March, J. (2022). Dealing With Radicalised Youth Offenders: The Development and Implementation of a Youth-Specific Framework. *Frontiers in psychiatry*, 12, 773545. <https://doi.org/10.3389/fpsy.2021.773545>
- Beršnak, J. V., & Prezelj, I. (2021). Recognizing youth radicalization in schools: Slovenian ‘frontline’ school workers in search of a compass. *International Sociology*, 36(1), 49–70.
- Bertelsen, P. (2015). Danish preventive measures and de-radicalization strategies: The Aarhus model. *Panorama: Insights into Asian and European Affairs*, 1(241), 53.
- Blakemore, S. J. (2018). Avoiding social risk in adolescence. *Current Directions in Psychological Science*, 27, 116–122.
- Borum, R. (2011). Radicalization into violent extremism I: A review of social science theories. *Journal of strategic security*, 4(4), 7–36.
- Borum, R., & Patterson, T. D. (2019). Juvenile radicalization into violent extremism: Investigative and research perspectives. *Journal of the American Academy of Child & Adolescent Psychiatry*, 58(12), 1142–1148. <https://doi.org/10.1016/j.jaac.2019.07.932>
- Bronsard, G., Cherney, A., & Vermeulen, F. (2022). Editorial: Radicalization Among Adolescents. *Frontiers in psychiatry*, 13, 917557. <https://doi.org/10.3389/fpsy.2022.917557>
- Bronsard, G., Cohen, D., Diallo, I., Pellerin, H., Varnoux, A., Podlipski, M. A., Gerardin, P., Boyer, L., & Campelo, N. (2022). Adolescents Engaged in Radicalisation and Terrorism: A Dimensional and Categorical Assessment. *Frontiers in psychiatry*, 12, 774063. <https://doi.org/10.3389/fpsy.2021.774063>
- Campelo, N., Oppetit, A., Neau, F., Cohen, D., & Bronsard, G. (2018). Who are the European youths willing to engage in radicalisation? A multidisciplinary review of their psychological and social profiles. *European psychiatry: the journal of the Association of European Psychiatrists*, 52, 1–14. <https://doi.org/10.1016/j.eurpsy.2018.03.001>
- Campelo, N., Oppetit, A., Thompson, C., Cohen, D., & Louet, E. (2022). A Clinical and Psychopathological Approach to Radicalization Among Adolescents. *Frontiers in psychiatry*, 13, 788154. <https://doi.org/10.3389/fpsy.2022.788154>
- Cherney, A. (2020). Exploring youth radicalisation through the framework of Developmental Crime Prevention: A Case Study of Ahmad Numan Haider. *Current Issues in Criminal Justice*, 32(3), 277–291. <https://doi.org/10.1080/10345329.2020.1784503>
- Dhami, M. K., & Murray, J. (2016). Male Youth Perceptions of Violent Extremism: towards a Test of Rational Choice Theory. *The Spanish journal of psychology*, 19, E51. <https://doi.org/10.1017/sjp.2016.49>
- Doosje, B., Loseman, A., & Van Den Bos, K. (2013). Determinants of radicalization of Islamic youth in the Netherlands: Personal uncertainty, perceived injustice, and perceived group threat. *Journal of Social Issues*, 69(3), 586–604.
- Doosje, B., Moghaddam, F. M., Kruglanski, A. W., De Wolf, A., Mann, L., & Feddes, A. R. (2016). Terrorism, radicalization and de-radicalization. *Current Opinion in Psychology*, 11, 79–84.
- Emmelkamp, J., Asscher, J.J., Wissink, I.B., & Stams, G.J. (2020). Risk factors for (violent) radicalization in juveniles: A multilevel meta-analysis. *Aggression and Violent Behavior*, 55, 101489. <https://doi.org/10.1016/j.avb.2020.101489>
- Erikson, E. H. (1968). *Identity: Youth and Crisis*. Norton, New York.
- García Coll, C., & Marks, A. K. (2017). Missing developmental and sociocultural perspectives: Comment on the “Psychology of Terrorism” special issue (2017). *American Psychologist*, 72(7), 701–702. <https://doi.org/10.1037/amp0000211>

- Hariz, B. (2021a, Feb 3). ISD adjusts its approach to rehabilitation as those dealt with for terror-linked conduct get younger. *The Straits Times*. <https://www.straitstimes.com/singapore/trend-of-younger-people-falling-prey-to-terrorist-ideology-has-isd-adjust-its>
- Hariz, B. (2021b, Feb 3). Self-radicalised youth went from ISIS supporter to star student with rehabilitation: ISD. *The Straits Times*. <https://www.straitstimes.com/singapore/self-radicalised-youth-went-from-isis-supporter-to-star-student-with-rehabilitation-isd>
- Heinke, D. H., & Persson, M. (2016). Youth Specific Factors in Radicalization. *Defence Against Terrorism Review*, 8, 53-66.
- Hogg, M. A. (2007). Uncertainty-identity theory. In M. P. Zanna (Ed.), *Advances in experimental social psychology*, Vol. 39, pp. 69–126. *Elsevier Academic Press*. [https://doi.org/10.1016/S0065-2601\(06\)39002-8](https://doi.org/10.1016/S0065-2601(06)39002-8)
- Hogg, M. A., Meehan, C., & Farquharson, J. (2010). The solace of radicalism: Self-uncertainty and group identification in the face of threat. *Journal of Experimental Social Psychology*, 46(6), 1061–1066. <https://doi.org/10.1016/j.jesp.2010.05.005>
- Human Rights Council. (2016). *Report on best practices and lessons learned on how protecting and promoting human rights contribute to preventing and countering violent extremism*. (Report No. A/HRC/33/29). Office of the United Nations High Commissioner for Human Rights. https://ap.ohchr.org/documents/dpage_e.aspx?si=A/HRC/33/29
- Institute for Economics & Peace. (2022). *Global Terrorism Index 2022: Measuring the Impact of Terrorism. Vision of Humanity*. <https://www.visionofhumanity.org/maps/global-terrorism-index/#/>
- Internal Security Department. (2021a). Singapore Terrorism Threat Assessment Report 2021. Ministry of Home Affairs. <https://www.mha.gov.sg/mediaroom/press-releases/singapore-terrorism-threat-assessment-report-2021/>
- Internal Security Department. (2021b, December 4). *20th Anniversary of ISD's Operations Against Jemaah Islamiyah in Singapore* [Press release]. <https://www.mha.gov.sg/mediaroom/press-releases/20th-anniversary-of-isd-operations-against-jemaah-islamiyah-in-singapore/>
- Internal Security Department. (2022a). *Update on Terrorism-Related Case Under Internal Security Act*. Ministry of Home Affairs. <https://www.mha.gov.sg/mediaroom/press-releases/update-on-terrorism-related-case-under-internal-security-act/>
- Internal Security Department. (2022b). *Singapore Terrorism Threat Assessment Report 2022*. Ministry of Home Affairs. <https://www.mha.gov.sg/mediaroom/press-releases/singapore-terrorism-threat-assessment-report-2022/>
- Koh, F. (2021a, Jan 27). 16-year-old detained under ISA for planning mosque attacks to receive religious, psychological counselling. *The Straits Times*. <https://www.straitstimes.com/singapore/16-year-old-detained-under-isa-for-planning-mosque-attacks-to-receive-religious>
- Koh, F. (2021b, Feb 3). ISD details terror suspects' rehabilitation for first time. *The Straits Times*. <https://www.straitstimes.com/singapore/terror-suspects-in-singapore-undergo-religious-psychological-and-social-rehabilitation-isd>
- Koh, F. (2021c, Feb 16). Parliament: Schools and institutes of higher learning among targets of youth outreach to combat radicalisation. *The Straits Times*. <https://www.straitstimes.com/singapore/politics/parliament-schools-and-institutes-of-higher-learning-among-targets-of-youth>
- Kruglanski, A. W., Bélanger, J. J., Gelfand, M., Gunaratna, R., Hettiarachchi, M., Reinares, F., Orehek, E., Sasota, J., & Sharvit, K. (2013). Terrorism—A (self) love story: Redirecting the significance quest can end violence. *American Psychologist*, 68(7), 559–575. <https://doi.org/10.1037/a0032615>
- Lefas, M., & Nozawa, J. (2016). Rehabilitating Juvenile Violent Extremist Offenders in Detention Advancing a Juvenile Justice Approach. *Global Center on Cooperative Security*. <http://www.jstor.org/stable/resrep20392>
- Martin, C. A., Kelly, T. H., Rayens, M. K., Brogli, B. R., Brenzel, A., Smith, W. J., & Omar, H. A. (2002). Sensation seeking, puberty, and nicotine, alcohol, and marijuana use in adolescence. *Journal of the American Academy of Child and Adolescent Psychiatry*, 41(12), 1495–1502. <https://doi.org/10.1097/00004583-200212000-00022>
- Oppetit, A., Campelo, N., Bouzar, L., Pellerin, H., Hefez, S., Bronsard, G., Bouzar, D., & Cohen, D. (2019). Do Radicalized Minors Have Different Social and Psychological Profiles From Radicalized Adults? *Frontiers in psychiatry*, 10, 644. <https://doi.org/10.3389/fpsy.2019.00644>

- Pels, T., & de Ruyter, D. J. (2012). The Influence of Education and Socialization on Radicalization: An Exploration of Theoretical Presumptions and Empirical Research. *Child & youth care forum*, 41(3), 311–325. <https://doi.org/10.1007/s10566-011-9155-5>
- Radicalisation Awareness Network. (2017). *Working with families and safeguarding children from radicalization: Step-by-step guidance paper for practitioners and policy-makers*. RAN YF&C and RAN H&SC. [https://home-affairs.ec.europa.eu/system/files_en?file=2020-09/ran_yf-c_h-sc_working_with_families_safeguarding_children_en.pdf](https://home-affairs.ec.europa.eu/system/files/en?file=2020-09/ran_yf-c_h-sc_working_with_families_safeguarding_children_en.pdf)
- Religious Rehabilitation Group. (2016). *Outreach Efforts*. RRG. <https://www.rrg.sg/outreach-efforts/>
- Robert, B. (2018). At-Risk and Radicalised Singaporean Youths: Themes Observed and Considerations for a Youth-Centric Rehabilitation Framework. In M. Khader, L. S. Neo, J. Tan, D. D. Cheong, & J. Chin (Eds.), *Learning from violent extremist attacks: Behavioural Sciences Insights for practitioners and policymakers* (pp. 239–257). World Scientific.
- Rolling, J., Corduan, G., Roth, M., Schroder, C. M., & Mengin, A. C. (2022). Violent Radicalization and Post-Traumatic Dissociation: Clinical Case of a Young Adolescent Girl Radicalized. *Frontiers in psychiatry*, 13, 793291. <https://doi.org/10.3389/fpsy.2022.793291>
- S. Rajaratnam School of International Studies (RSIS). *CENS Workshop on Life Psychological Intervention*. Nanyang Technological University. <https://www.rsis.edu.sg/event/cens-workshop-on-life-psychological-intervention/>
- Schmid, A. P. (2013). Radicalisation, de-radicalisation, counter-radicalisation: A conceptual discussion and literature review. *ICCT Research Paper*, 97(1), 22.
- Schröder, C. P., Bruns, J., Lehmann, L., Goede, L. R., Bliesener, T., & Tomczyk, S. (2022). Radicalization in Adolescence: The Identification of Vulnerable Groups. *European Journal on Criminal Policy and Research*, 1-25.
- SGSecure (2019). *SGSecure: Home*. Government of Singapore. <https://www.sgsecure.gov.sg/>
- Shanmugam, K. (2021). *Written Reply to Parliamentary Question on Engaging Youths on the Ills of Radicalisation, by Mr K Shanmugam, Minister for Home Affairs and Minister for Law*. Ministry of Home Affairs. <https://www.mha.gov.sg/mediaroom/parliamentary/written-reply-to-parliamentary-question-on-radicalisation-of-foreign-domestic-workers-by-mr-k-shanmugam-minister-for-home-affairs-and-minister-for-law/>
- Siegel, A., Brickman, S., Goldberg, Z., & Pat-Horenczyk, R. (2019). Preventing future terrorism: Intervening on youth radicalization. *Integrating Psychiatry and Primary Care*, 391–418. https://doi.org/10.1007/978-3-030-15872-9_19
- Silvers, J. A., McRae, K., Gabrieli, J. D., Gross, J. J., Remy, K. A., & Ochsner, K. N. (2012). Age-related differences in emotional reactivity, regulation, and rejection sensitivity in adolescence. *Emotion*, 12, 1235–1247. <https://doi.org/10.1037/a0028297>
- Steinberg L. (2008). A Social Neuroscience Perspective on Adolescent Risk-Taking. *Developmental review: DR*, 28(1), 78–106. <https://doi.org/10.1016/j.dr.2007.08.002>
- T'ng, K. (2019). Down the Rabbit Hole: ISIS on the Internet and How It Influences Singapore Youth. *Home Team Journal*, 1(8), 40–47.
- Tuen, A. (2021). *A Battle for Hearts and Minds*. Ministry of Home Affairs. <https://www.mha.gov.sg/careers/home-team-news/story/detail/a-battle-for-hearts-and-minds>
- Van San, M., Sieckelinck, S., & De Winter, M. (2013). Ideals adrift: An educational approach to radicalization. *Ethics and Education*, 8(3), 276-289.
- Ventriglio, A., & Bhugra, D. (2019). Identity, alienation, and violent radicalization. In D. Marazziti, & S. M. Stahl (Eds.), *Evil, terrorism and psychiatry* (pp. 17–29). Cambridge University Press. <https://doi.org/10.1017/9781108569095.005>
- Zych, I., & Nasaescu, E. (2021). PROTOCOL: Is radicalization a family issue? A systematic review of family-related risk and protective factors, consequences, and interventions against radicalization. *Campbell Systematic Reviews*, 17(3), e1190.

DRUG TRAFFICKING

DEVELOPMENTS IN THE ILLICIT DRUG MARKET IN EAST AND SOUTHEAST ASIA

Regional Office for Southeast Asia and the Pacific (Bangkok)
United Nations Office on Drugs and Crime

ABSTRACT

The illicit drug market in East and Southeast Asia has changed dramatically in recent years, marked by unprecedented growth in manufacture and trafficking of synthetic drugs, particularly methamphetamine. In 2021, the 10 ASEAN countries, China, Japan and the Republic of Korea all reported methamphetamine as their primary drug of concern, while it was the case for only six of these countries a decade ago. At the same time, sizeable amounts of opium continue being cultivated in Shan State, Myanmar, to supply the regional heroin market. Several concerning developments have been observed in the illicit drug market in East and Southeast Asia. Prices of methamphetamine have continued decreasing while seizures of the drug have increased every year over the last decade. Together with no significant change in purities of methamphetamine, this trend strongly indicates the wide availability of the drug in the region. Another concerning development is the extremely low level of precursor chemical seizures, required for the illicit manufacture of methamphetamine and heroin. Fundamentally, the surge in the illicit manufacture of methamphetamine is not possible without two underlying conditions: a steady supply of chemicals and growing demand for methamphetamine. In East and Southeast Asia, there is significantly limited data on drug use, which makes it difficult to understand the extent of drug demand. Moreover, national authorities in the region have not been able to successfully disrupt diversion and trafficking of chemicals nor the equipment required for the illicit manufacture of methamphetamine. Regional cooperation measures to address challenges associated with drugs and chemicals are already in place, but there is much room for improvement. In particular, governments must enhance their understanding of non-controlled chemicals that can be used for the illicit manufacture of drugs and the need for stronger cooperation ties amongst them. It would also be beneficial for governments to invest more resources to develop accurate data and information on drug demand.

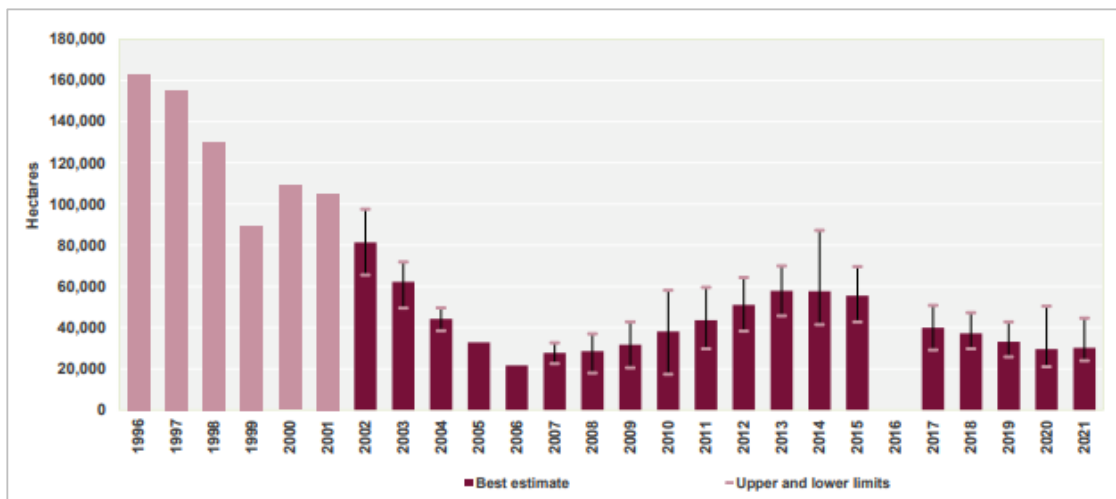
INTRODUCTION

In recent years, illicit drug markets around the world have experienced a rapid growth of the synthetic drug market. East and Southeast Asia are not immune to this development as there has been a significant surge in supply of methamphetamine over the last decade. Although heroin remains of concern in the region, the flexibility of synthetic drug manufacture has resulted in an expansion of the synthetic drug market, especially for methamphetamine. East and Southeast Asia are now home to one of the world's largest markets for methamphetamine, with record amounts being seized year on year, and several countries in the region have featured in the top ten countries for global methamphetamine seizures.

Although drug control strategies are in place, efforts to disrupt drug trafficking and production are impeded by the region's porous borders and constant evolution of, not only the substances available in the market, but also the versatility of their manufacture. Non-controlled chemicals are increasingly being used for synthetic drug production, and lowered manufacturing costs have resulted in organised crime groups being able to lower prices and drive methamphetamine supply and demand in the region.

This article will delve into recent concerning developments in three key drug markets in East and Southeast Asia, namely heroin, methamphetamine, and ketamine, and propose recommendations to address the growing drug challenges in the region.

Figure 1. Opium poppy cultivation in Myanmar (in hectares), 1996-2021



Source: UNODC, Myanmar Opium Survey 2021: Cultivation, Production, and Implications, April 2022.

HEROIN

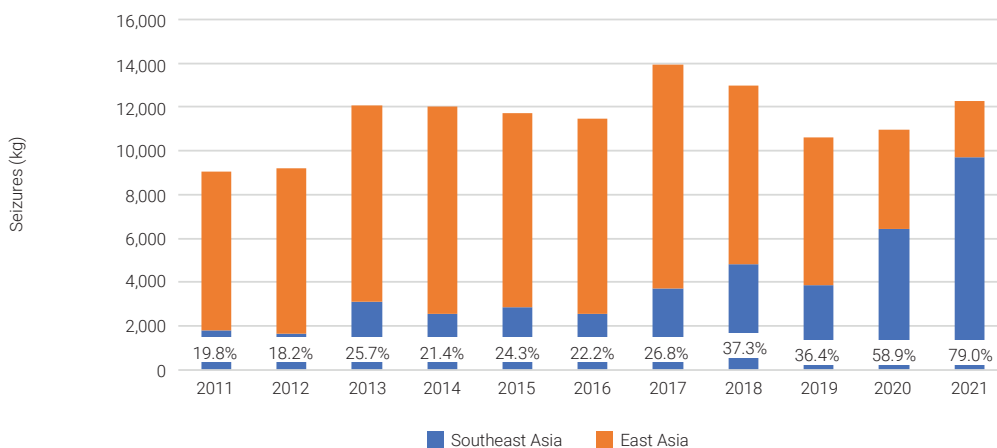
Persistent Challenges Posed by Heroin

Prior to the escalation of the supply and demand of methamphetamine in East and Southeast Asia, heroin was the main primary drug of concern, and though its presence has since diminished, it still remains an important drug in the region and there are indications of its potential resurgence in the past year.

Myanmar, as the second largest producer of opium in the world, behind Afghanistan, remains a

main source of heroin in the region.¹ In 2021, the area under opium poppy cultivation in Myanmar increased for the first time since 2014, from an estimated 29,550 hectares in 2020 to 30,200 hectares in 2021 (see Figure 1). While the increase is small, the change in trend indicates the possibility of returning opium poppy cultivation and a resurgence of heroin production within the country.

Indeed, the rise in opium cultivated in Myanmar has been met with a similar rise in the amount of heroin seized in the country, from 1.9 tons in 2020 to a record 2.5 tons in 2021. This has also affected neighbouring countries in the region.



¹ Within the region, Lao PDR also has areas under opium poppy cultivation, however, information on recent cultivation trends in the country is limited.

Although the total amount of heroin seized in East and Southeast Asia has seen no significant change over the past decade, in recent years quantities of the drug trafficked to Southeast Asia have significantly increased at the expense of East Asia (see Figure 2). In 2021, nearly 12.3 tons of heroin were seized in the region, compared to the 10.9 tons in 2020, with Southeast Asia accounting for 79% (9.7 tons) of the total amount seized. This reflects changes in drug trafficking routes for heroin in recent years, with organised crime groups increasingly targeting lower Mekong countries as major transit and destination points rather than China, which has seen a decline in heroin seizures from 9.5 tons in 2017 to only 1.8 tons in 2021. Aside from Myanmar, Thailand and Malaysia also reported record seizures of heroin in 2021 (3.4 tons and 2.2 tons respectively). Singapore has also seen an increase in the amount of heroin seized in recent years. Though not as large a volume as other countries in the region, Singapore seized 95.4 kg of heroin in 2021 (Central Narcotics Bureau, 2022) – also a record for the country.

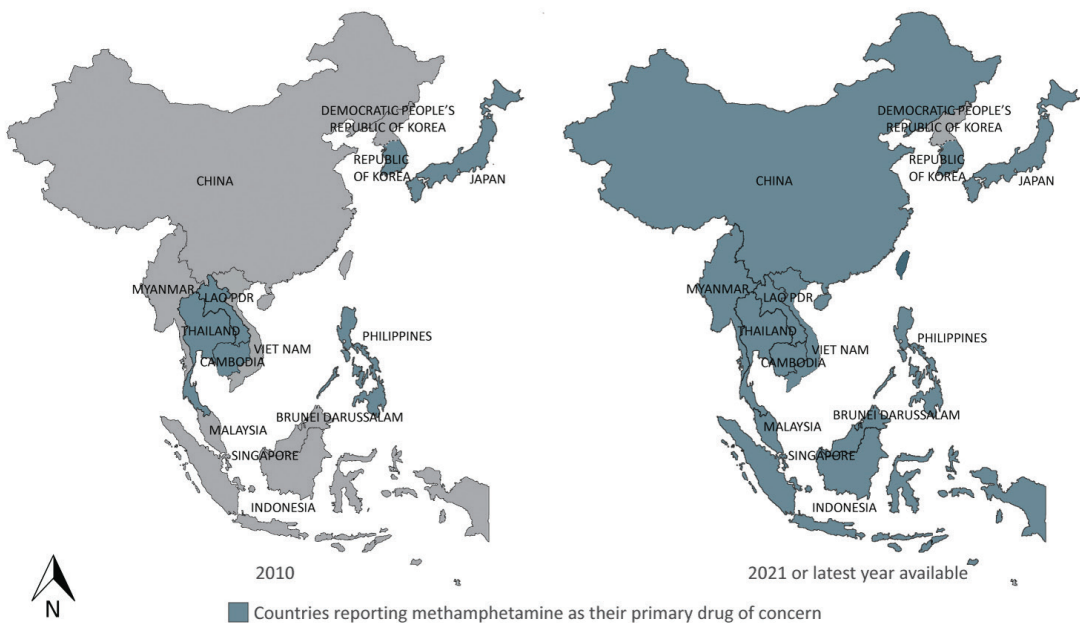
METHAMPHETAMINE

Continued Expansion of Methamphetamine Market in East and Southeast Asia

While heroin has a continued presence in the region, it is undeniable that over the past decade, there has been a drastic shift in the drug market in East and Southeast Asia towards methamphetamine. In 2010, of the 13 countries in the region (viz. the ASEAN member states, China, Japan and the Republic of Korea), only six countries (Thailand, Lao PDR, the Philippines, Brunei Darussalam, the Republic of Korea, and Japan) reported methamphetamine as their primary drug of concern. However, as of 2021, all 13 countries now report their primary drug of concern to be methamphetamine.

This is also reflected in the amount of methamphetamine seized in the region, which has continually increased over the past decade, despite developments such as the COVID-19 pandemic and the recent political upheaval in

Map 1. Countries in East and Southeast Asia reporting methamphetamine as their primary drug of concern, 2010 and 2021 (or latest year available)



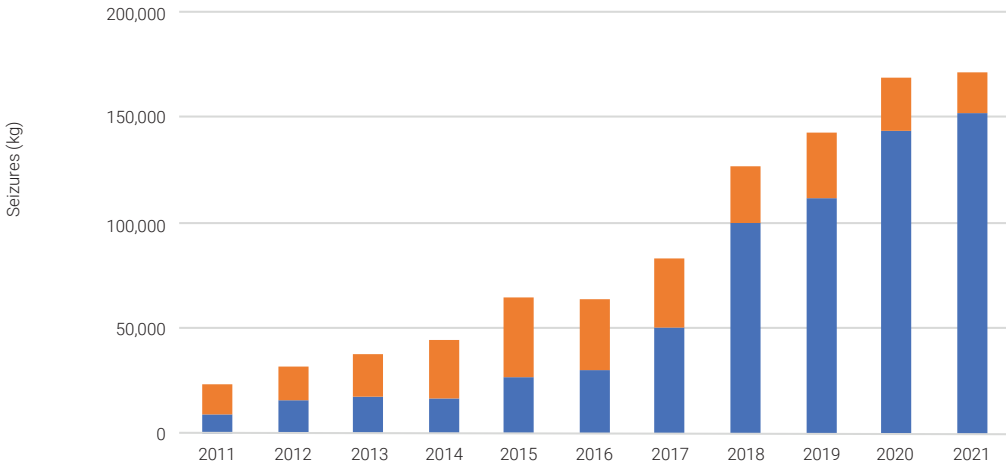
The boundaries and names shown and the designations used on this map do not imply official endorsement or acceptance by the United Nations.

Source: UNODC, *Synthetic Drugs in East and Southeast Asia: Latest developments and challenges*, May 2022.

Myanmar following the coup in February 2021, showing the resilience of organised crime in the region to continue to push the supply of methamphetamine into the market. In 2021, a total of 171.6 tons of methamphetamine was seized in East and Southeast Asia, with Southeast Asia (and particularly the lower Mekong subregion countries

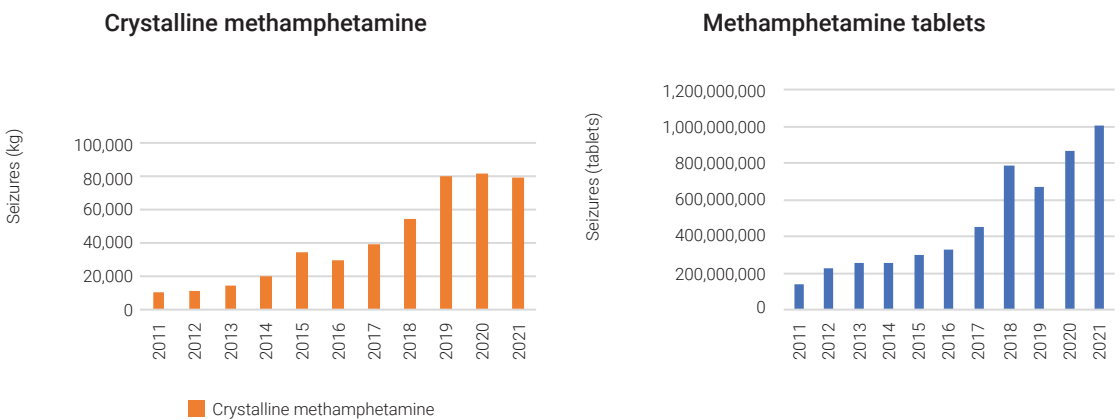
of Cambodia, Lao PDR, Myanmar, Thailand and Vietnam) accounting for nearly 90% of total seizures, including a record amount of methamphetamine tablets (see Figure 3). For the first time, East and Southeast Asia seized a combined total of over one billion methamphetamine tablets, weighing approximately 90.6 tons (see Figure 4).

Figure 3. Seizure amounts of methamphetamine in East and Southeast Asia, by region, 2011-2021



Sources: DAINAP; UNODC, Responses to the Annual Report Questionnaire (ARQ); UNODC official communication with national drug agencies in the region, February-August 2022.

Figure 4. Seizures of methamphetamine tablets and crystalline methamphetamine, 2011-2021



Sources: Drug Abuse Information Network for Asia and the Pacific (DAINAP); UNODC, Responses to the ARQ; UNODC official communication with national drug agencies in the region, February-May 2022.

In Southeast Asia, the amount of methamphetamine seized increased from 143.5 tons in 2020 to 152 tons in 2021. Although there was a substantial decrease in the amount of methamphetamine seized in Myanmar from 49 tons in 2020 to 31.9 tons in 2021, this was more than offset by increases in the amount of methamphetamine seized in neighbouring countries, including Lao PDR and Thailand, which both seized a record amount of methamphetamine – 75.4 tons and 15.8 tons respectively (UNODC, 2022). In the maritime Southeast Asian countries of Brunei Darussalam, Indonesia, Malaysia, the Philippines, and Singapore, only Brunei Darussalam and Malaysia did not report an increase in seizures in 2021. It is important to note that in the case of Malaysia, the decline was due to a significant drop in the amount of liquid methamphetamine seized (from 6 tons in 2020 to 188.5 kg in 2021). However, record amounts of both crystalline methamphetamine and methamphetamine tablets were seized in the country, further signifying that there was a spill-over of methamphetamine from Myanmar to other countries in the region (UNODC, 2022).

Meanwhile, in East Asia, the amount of methamphetamine seized dropped from 25.7 tons in 2020 to 19.6 tons in 2021, despite increases in Japan, the Republic of Korea, and Hong Kong, China. The large drop can be attributed to a decline in seizures in China, which seized 6.2 tons less of methamphetamine in 2021 than the previous year (Drug Abuse Information Network for Asia and the Pacific [DAINAP] data).

Consolidation of Methamphetamine Production in Shan State, Myanmar

The factor primarily contributing to the converse relationship between the quantity of methamphetamine seized in East Asia and Southeast Asia, as well as its continued increase, is the shift in methamphetamine production sites from China to Shan State, Myanmar, since around 2015. Shan State has now become the epicentre of methamphetamine manufacture in the region (UNODC, 2019). It is home to several non-state armed groups which have worked together with organised crime to successfully engineer the expansion of the synthetic drug market in the region.

This is evidenced by the seizure of chemicals that can be used to illicitly manufacture

methamphetamine within and en route to production sites in Shan State, the forensic profiles of methamphetamine seized, as well as the trademark Chinese teabag packages used to conceal crystalline methamphetamine manufactured in Myanmar, that are found across the region and beyond, including in Australia and New Zealand. Though there are a variety of packages, the most commonly detected are labelled with names such as “Guanyinwang”, “Qing Shan”, “Pin Wei”, and “Da Guan Yin” (see Figure 5).

Figure 5. Major teabag packages found in Southeast Asia



Sources: National Anti-Drug Agency (NADA) of Malaysia, CCDAC of Myanmar, and Philippine Drug Enforcement Agency (PDEA) of the Philippines.

Similarly, methamphetamine tablets manufactured in the Golden Triangle of Myanmar are also commonly detected with branding marks. These include “999”, “Y1” and “1” or “2”. An interesting development in 2021, together with the surge in methamphetamine tablets, is the wider variety of branding marks on tablets seized by authorities in Thailand. Whereas in 2020 only 2.8% of the seized methamphetamine tablets bore packaging marked with other branding, in 2021, the proportion increased to 13.0% (see Table 1). While information is limited, available intelligence from drug control authorities in the region suggests

Table 1. Proportion of different branding on methamphetamine tablet packaging seized in Thailand, 2020-2021

Branding	2020	2021
“999”	76.2%	73.5%
“Y1”	20.0%	13.2%
“1” or “2”	0.5%	0.1%
Other branding	2.8%	13.0%
No logo	0.5%	0.3%

that there are links between branding marks and the non-state armed groups or organised crime groups which manufactured or tableted the drug (UNODC, 2022). The increase in “other” branding may indicate that more groups were involved in the production of methamphetamine tablets in 2021.

Trafficking Routes Within East and South Asia and Growing Interregional Links

Methamphetamine produced in Myanmar is trafficked through many different border points, and through various means, before reaching their destination markets in East and Southeast Asia, Oceania, and South Asia.

One of the notable developments in 2021 in trafficking routes is that Lao PDR has been increasingly targeted for methamphetamine trafficking. Due to intensified law enforcement operations along the northern border between Thailand and Myanmar, especially following the

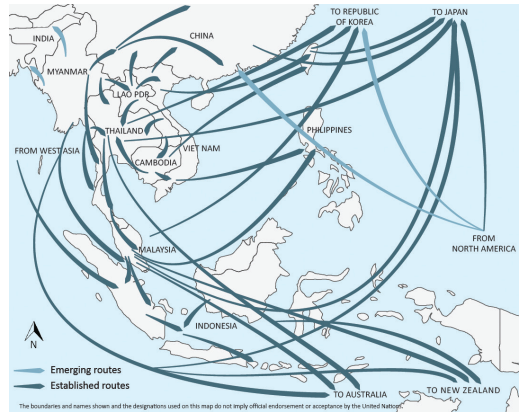
Map 2. Methamphetamine tablet trafficking flows in the Mekong region, 2021



Source: UNODC, *Synthetic Drugs in East and Southeast Asia: Latest developments and challenges*, May 2022.

Note: Flow arrows represent the general direction of trafficking and do not coincide with precise sources of production or manufacture, are not actual routes and are not weighed for significance or scale. Boundaries, names and designations used do not imply official endorsement or acceptance by the United Nations.

Map 3. Crystalline methamphetamine trafficking flows in East and Southeast Asia, 2021



Source: UNODC, *Synthetic Drugs in East and Southeast Asia: Latest developments and challenges*, May 2022.

Note: Flow arrows represent the general direction of trafficking and do not coincide with precise sources of production or manufacture, are not actual routes and are not weighed for significance or scale. Boundaries, names and designations used do not imply official endorsement or acceptance by the United Nations.

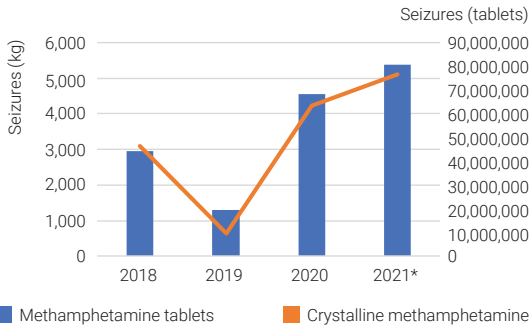
COVID-19 outbreak and ensuing implementation of mobility-associated restrictions, it appears that drug traffickers have opted to reroute methamphetamine through Lao PDR for further trafficking to Thailand, Cambodia, and Vietnam.

This is evidenced by the drastic increase in methamphetamine tablets seized in Lao PDR from 2021 onwards, as well as increased seizures along Thailand’s northeastern border with Lao PDR (see Figure 6). The amount of methamphetamine tablets seized in Lao PDR increased by 669% from 18 million tablets in 2020 to over 143 million tablets in 2021, including a massive seizure of 55.6 million tablets and 1,537 kg of crystalline methamphetamine in October 2021 in Bokeo province, bordering Myanmar and Thailand – a record amount for the region.² This trend has continued into 2022, with several additional large seizures in and around Bokeo province including 36.5 million tablets and 590 kg of crystalline methamphetamine in January, and 33 million tablets and 500 kg of crystalline methamphetamine in September.³ Available intelligence also suggests that tableting operations in Lao PDR are ongoing.

² Official communication with Lao National Commission for Drug Control and Supervision (LCDC), March 2022.

³ Communication with LCDC, September 2022.

Figure 6. Seizure amounts of methamphetamine in northeastern Thailand, 2018-2021



Source: Official communication with ONCB of Thailand, May 2022. (*Data for 2021 are preliminary.)

Another notable development is organised crime taking advantage of the porous borders between Myanmar and India to intensify trafficking of both methamphetamine tablets and crystalline methamphetamine into India. Over the past year, increasing amounts of methamphetamine have been seized in the northeastern region of India bordering Myanmar. These include seizures of 100,000 methamphetamine tablets in November and 154 kg of crystalline methamphetamine in December 2021 (Karimganj Police, 2021). With an already established market for methamphetamine in Bangladesh, the large population in India is another attractive target for organised crime to expand their operations further westward in South Asia.

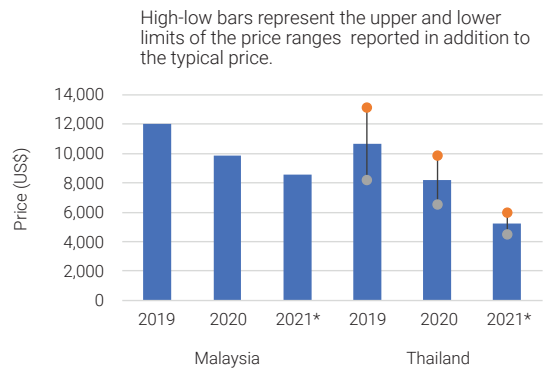
Decreasing Prices of Methamphetamine

Prices for methamphetamine tablets and crystalline methamphetamine have continued to decrease in recent years while purities remain stable. This is concerning as it means that, despite record seizures of the drug every year, there is still an abundance of methamphetamine in the market. Organised crime groups have been able to achieve economies of scale – lowering production costs while simultaneously increasing production capacity to flood the market with methamphetamine.

Methamphetamine tablets can be found for as low as US\$1 in Cambodia and in some areas in Thailand, especially near the border with Myanmar. Retail and wholesale prices for crystalline methamphetamine also show a decline. Available data from Malaysia and Thailand, which are key transit and destination

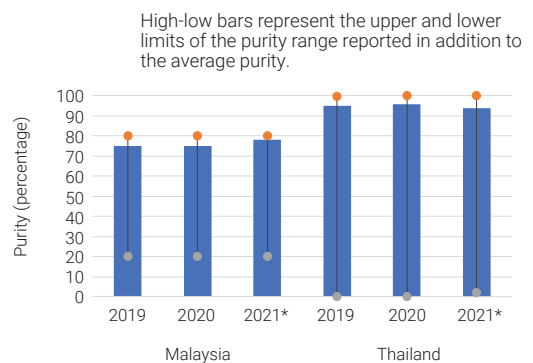
countries for the drug, show that wholesale prices have dropped in the past two years, from US\$12,000 in 2019 to US\$8,595 in 2021 in Malaysia, and from US\$10,656 to US\$5,208 in Thailand (see Figure 7). Meanwhile, the purity of the drug remains high (see Figure 8), meaning increased affordability and accessibility to high-quality crystalline methamphetamine. Overall, the price of methamphetamine across Southeast Asia is roughly one third of prices recorded a decade ago, according to data recorded by DAINAP.

Figure 7. Wholesale price of crystalline methamphetamine in Malaysia and Thailand, 2019-2021* (US\$)



Sources: Official communication with the National Anti-Drug Agency (NADA) of Malaysia, and ONCB of Thailand, March-May 2022. (*Data for 2021 are preliminary.)

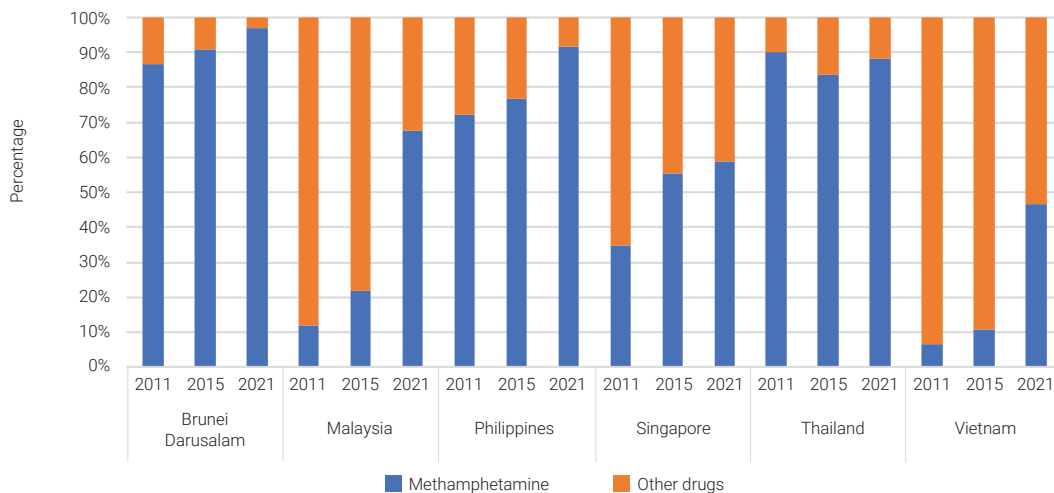
Figure 8. Purity of crystalline methamphetamine in Malaysia and Thailand, 2019-2021*



Sources: Official communication with NADA of Malaysia and ONCB of Thailand, March-May 2022. (*Data for 2021 are preliminary.)

Note: Purity data for Thailand refer to the weight/weight (w/w) percentage, expressed as the hydrochloride salt of these substances. For Malaysia, it refers to the weight/weight (w/w) percentage, expressed as the base form of these substances.

Figure 9. Proportion of methamphetamine users among all drug users as identified through various demand indicators in Brunei Darussalam, Malaysia, the Philippines, Singapore, Thailand, and Vietnam, 2011, 2015 and 2021



Sources: Official communication with the Narcotics Control Bureau (NCB) of Brunei, NADA of Malaysia, DDB of the Philippines, the Central Narcotics Bureau (CNB) of Singapore, ONCB of Thailand, and the Standing Office on Drugs and Crime (SODC) of Vietnam, February-May 2022.

Note: Data for Brunei Darussalam and Singapore are based on the number of drug users brought into formal contact with authorities; the data for Malaysia, the Philippines, and Thailand are based on treatment; and the data for Vietnam are based on registered drug users.

The impact of increased methamphetamine supply and reduced prices on demand for the drug can be observed from various drug demand indicators. Since 2011, there has been a rising proportion of drug users treated, or under formal contact with law enforcement authorities, for methamphetamine use at the expense of heroin (see Figure 9). For example, Malaysia and Vietnam, which were traditionally known for its sizeable heroin user base have seen an increasing number of methamphetamine users.

However, while these metrics can help paint a picture of shifting patterns in drug use, it is important to note that the data is limited, and it is likely that the demand for methamphetamine in the region has been severely underestimated, especially taking into account the large, escalating volumes of methamphetamine that are produced and trafficked within the region.

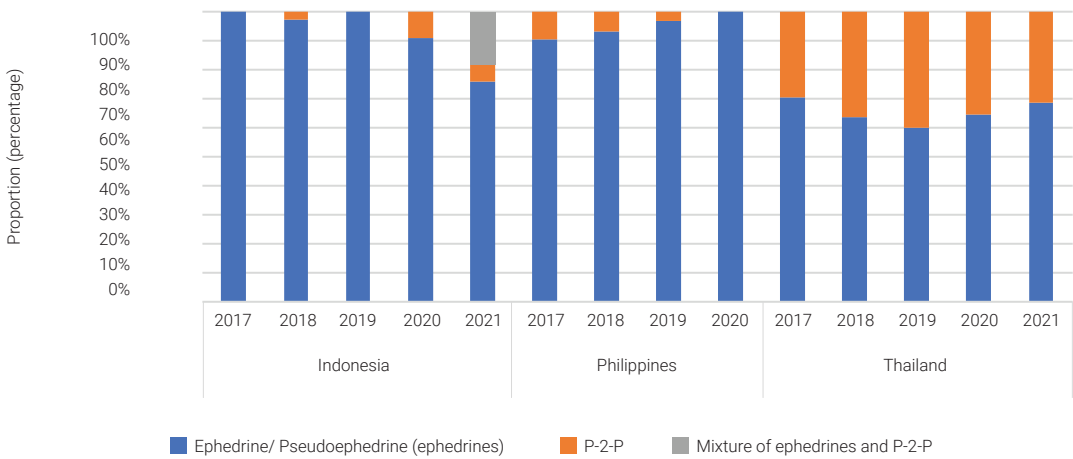
Precursors and Non-Controlled Chemicals

Despite large volumes of methamphetamine being seized every year, there have been significantly

limited seizures of its key precursors, such as ephedrine/pseudoephedrine (ephedrines) and P-2-P. Forensic analysis confirms that ephedrines-based manufacturing methods remain the primary synthesis routes for methamphetamine found in the region, with P-2-P also found to be used, though to a lesser extent (see Figure 10). However, practically no ephedrine/pseudoephedrine or P-2-P was seized in 2021, with only 6 kg of ephedrine seized in the Philippines and no P-2-P seized at all (see Figures 11 and 12).

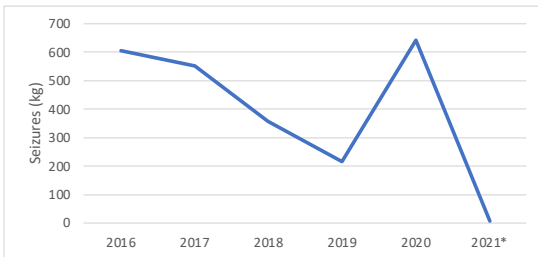
The incommensurate amount of the key precursors seized could in part be attributed to rising use of chemicals which are not internationally controlled under the 1988 United Nations Convention against Illicit Traffic in Narcotic Drugs and Psychotropic Substances, to produce not only methamphetamine, but also to synthesise the key precursors. In recent years, chemicals such as propionyl chloride, which can be used to produce ephedrine, and benzyl cyanide, which can be used to produce P-2-P, have been found at or en route to suspected methamphetamine production sites. The convergence between licit and illicit chemical

Figure 10. Proportion of crystalline methamphetamine samples analysed in Indonesia, the Philippines, and Thailand, by main precursor, 2017-2021*



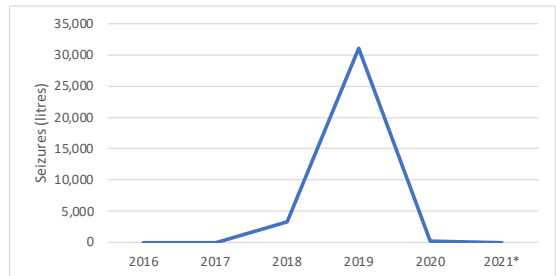
Sources: Official communication with the National Narcotics Board (BNN) of Indonesia, the Philippines Drug Enforcement Agency (PDEA) of the Philippines, and ONCB of Thailand, May 2022.
 (*Where 2021 data are not available, the latest year is shown. Data reported as “unknown” are not included here.)

Figure 11. Seizure amounts of ephedrine and pseudoephedrine (raw material) in Southeast Asia, 2016-2021



Source: DAINAP (*Data for 2021 are preliminary)

Figure 12. Seizure amounts of P-2-P in Southeast Asia, 2016-2021



Source: DAINAP (*Data for 2021 are preliminary)

trade adds further complexity to a region where efforts to prevent and divert precursor trafficking are already uneven and limited.

KETAMINE

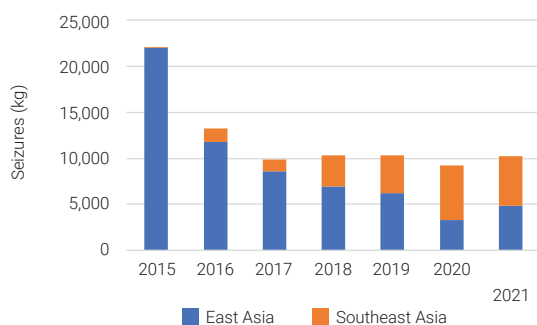
Growing Non-Medical Use of Ketamine and Drug Products Containing the Substance in Southeast Asia

In addition to methamphetamine, another synthetic drug which should be monitored closely, particularly in Southeast Asia, is ketamine. Though ketamine is not an internationally controlled substance and is listed as an essential medicine

by WHO, it is used as a recreational drug and is illicitly manufactured in the region, as well as sourced from outside the region, particularly from Pakistan.

In 2021, quantities of ketamine seized in the region amounted to 10.3 tons, marking an 11% increase compared to the preceding year, but 13 tons lower than 2015, the year when China alone seized 19.6 tons of the drug. However, similarly to methamphetamine, seizures of ketamine in Southeast Asia have increased significantly since 2015, rising from merely 83 kg to 5.4 tons in 2021 (see Figure 13).

Figure 13. Seizure amounts of ketamine in East and Southeast Asia, 2016-2021



Sources: DAINAP; UNODC, responses to the ARQ; Official communication with national drug agencies in the region, February-May 2022; Taiwan Ministry of Justice

Countries in the region also continue to report drug products containing ketamine in mixture with other substances. These products include “k-powdered milk”, which was found to be responsible for 13 drug overdose deaths in Thailand in January 2021. Autopsy results showed varying combinations of ketamine, diazepam, and caffeine in the mixture, as shown in Table 2.¹¹

Table 2. Forensic profile of “K-powdered milk” analysed in Thailand, 2021

Number of samples	Forensic profile of “K-powdered milk”
7	Diazepam, 12-99% diazepam purity
5	Diazepam and ketamine, 18-99% diazepam purity
4	Ketamine hydrochloride and caffeine, 13-24% ketamine purity

Source: Official communication with ONCB of Thailand, March 2021.

Another product is “happy water”. In April 2022, authorities in Thailand issued a warning for the emergence of “happy water” in the drug market; it was being sold online and at entertainment venues (Department of Medical Services, n.d.) in powder form in packets, which could be mixed in water or other drinks. Forensic analysis showed that ketamine was also one of the substances found in the product (see Table 3). Since then, similar packets have also been found in Myanmar (Central Committee for Drug Abuse Control, 2022). While

Table 3. Forensic profile of “happy water” analysed in Thailand, 2022

Group	Samples	Composition	Purity (per cent)
1	4	MDMA Ketamine	7.89 – 15.98 19.54 – 65.10
2	1	MDMA Nimetazepam	11.83 0.46
3	4	Methamphetamine Diazepam	35.01 – 46.18 16.98 – 24.59
4	2	MDMA Ketamine Caffeine	1.79 – 2.26 2.59 – 5.40 No quantitative
5	5	MDMA Ketamine Nimetazepam	3.78 – 33.47 1.32 – 55.34 0.17 – 0.47
6	3	MDMA Ketamine Caffeine Nimetazepam Lidocaine	2.92 – 4.13 0.25 – 1.24 No quantitative 0.21 – 0.34 No quantitative

Source: Official communication with ONCB of Thailand, September 2022.

¹¹Official communication with Office of the Narcotics Control Board (ONCB) of Thailand, March 2021.

no overdoses have been associated with the use of “happy water” thus far, the variance in mixtures and high content of dangerous substances present a potential public health risk.

Expansion of Illicit Ketamine Manufacture into Cambodia

While ketamine manufacture continues in Shan State, Myanmar, it appears that transnational organised crime groups are expanding their production operations and increasingly targeting Cambodia for synthetic drug production, especially for ketamine. As previously noted, Cambodian authorities seized nearly 2.8 tons of ketamine in 2021. This is an exponential increase compared to previous years, amounting to nearly fifteen times the amount seized in the previous five years combined (see Figure 14).

Figure 14. Seizure amounts of ketamine in Cambodia, 2016-2021

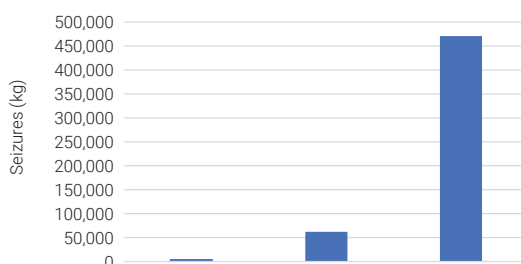


Source: Official communication with National Authority for Combating Drugs (NACD) of Cambodia, March 2022.

This increase is, in large part, due to emerging ketamine production in the country. In December 2021, an industrial-scale clandestine ketamine laboratory was dismantled in Kampong Speu province, where 2.5 tons of ketamine were seized along with 61.7 tons of various chemicals that could have been used not only for the production of ketamine but also other synthetic drugs. Additional laboratories for synthetic drug production, not limited to ketamine, were dismantled in January, May, and July of 2022 along with chemical storage facilities containing massive amounts of controlled and non-controlled chemicals. These chemicals

included ammonia and activated carbon, which can be used in ketamine manufacture, as well as acetic anhydride, benzoic acid, and cyclohexane, which can be used in the manufacture of other synthetic drugs. In sum, between September 2020 and July 2022, a total of 538 tons of chemicals were seized in the country, primarily in Kampong Speu, Phnom Penh, Svay Reang, and Sihanoukville (see Figure 15). Sophisticated laboratory equipment were also seized in the country during the period.⁴

Figure 15. Seizure amounts of controlled and non-controlled chemicals in Cambodia, 2020-2022



Source: Official communication with NACD of Cambodia, September 2022. (*Data for 2022 are for Jan-July.)

RECOMMENDATIONS

To address the evolving synthetic drug situation and the ensuing security and public health challenges, UNODC has the following recommendations:

1. **Strengthening of regional cooperation measures and expansion of interregional cooperation:** While regional cooperation measures already exist, in light of the spill-over of methamphetamine and other synthetic drugs in East and Southeast Asia to neighbouring regions, it is imperative that these measures are strengthened and interregional links are established so that information can be more easily exchanged and operations can be conducted across regional borders.
2. **Development of national strategies and action plans to deal with organised crime:** As organised crime groups have driven the expansion of the methamphetamine market in the region and have infiltrated licit businesses, such as the chemical trade, to do so, it is crucial for drug

⁴ Official communication with Office of the Narcotics Control Board (ONCB) of Thailand, March 2021.

control strategies to target organised crime operations and their proceeds of crime, including by adopting measures for in-depth investigation and addressing illicit financial flows.

understanding of the various chemicals used in illicit drug production, including their detection, safe handling, and disposal, especially among frontline officers.

- 3. Enhancing understanding of internationally controlled and non-controlled chemicals:** A key reason for the escalating production of the methamphetamine and other synthetic drugs in East and Southeast Asia is the proximity to large chemical industries and the insufficient measures in place to disrupt the diversion and trafficking of chemicals in the region. With the increasing use of non-controlled chemicals, it is even more important to build a greater
- 4. Collection and sharing of data/information:** With the constant evolution of the synthetic drug market, robust data collection and sharing systems are needed to keep abreast of emerging trends and support the formulation of evidence-based policies and legislative measures. This includes developing more accurate data and information on drug demand, to better understand the scale of drug use and changing drug use patterns in the region.

ABOUT THE AUTHOR

For two decades, the **United Nations Office on Drugs and Crime (UNODC)** has been helping make the world safer from drugs, organised crime, corruption and terrorism. It is committed to achieving health, security and justice for all by tackling these threats and promoting peace and sustainable well-being as deterrents to them. UNODC's Regional Office for Southeast Asia and the Pacific is located in Bangkok, Thailand, and this article is contributed by the Drug and Precursor Team of the Regional Office.

More information about UNODC is available at its website:
<https://www.unodc.org/unodc/en/about-unodc/index.html>

REFERENCES

Central Committee for Drug Abuse Control (CCDAC), Myanmar. (2022, June 3). *Over K170 min worth of ecstasy and ketamine seized in Yangon Region and Kayin State*. Retrieved from www.facebook.com/CCDACMyanmar/posts/pfbid0uJ3v7H5jJKNd6oXjDEUsyr4E47tkvFZXDMkwgo4ahu1t3jAR7VwVbtzLLscBKorvl.


Central Narcotics Bureau. (2022, June 10). *Overview of Singapore's Drug Situation in 2021*. Retrieved from www.cnb.gov.sg/docs/default-source/drug-situation-report-documents/cnb-annual-statistics-2021-final.pdf.

Department of Medical Services, Thailand. (n.d.). Retrieved from www.dms.go.th/Content/Select_Landing_page?contentId=33127.

Dimapur Police, India. (2022, February 16). *Drugs worth approx ₹5 CRORE seized. In a major breakthrough Special Operations Team of #dimapurpolice seized Huge quantities of Yaba (World is Yours) tablet. Two Drug Smugglers arrested. Case under investigation*. Retrieved from twitter.com/dimapurpolice/status/1493954525681831938.

Karimganj Police, India. (2021, November 17). *In a successful operation, a team of Veterbond AD camp under Ratabari PS recovered a huge consignment of 100,000 YABA tablets worth 3 crores which was on the way from Aizawl. 1 arrested and an Innova detained*. Retrieved from twitter.com/karimganjpolice/status/1460948185195560967.

Taiwan Ministry of Justice. (n.d.). *Drug Offenses (Monthly)*. Retrieved from www.moj.gov.tw/2832/2833/2853/2854/2857/.



United Nations Office on Drugs and Crime. (2022, May). *Synthetic Drugs in East and Southeast Asia: Latest developments and challenges (2022)*.

United Nations Office on Drugs and Crime. (2022, April). *Myanmar Opium Survey 2021: Cultivation, Production, and Implications*.

United Nations Office on Drugs and Crime. (2019, July). *Transnational Organized Crime in Southeast Asia: Evolution, Growth and Impact (2019)*.

CYBERCRIMINALS AND COVID-19 SCAMS

Mkay Bonner & Mark S. Johnson
University of Louisiana Monroe, United States of America

ABSTRACT

Around the world, the COVID-19 pandemic has provided cybercriminals with unprecedented opportunities to take advantage of the weak and defenceless. Part 1 of this essay discusses the cognitive vulnerabilities that increase susceptibility to scams, particularly for teenagers, persons with a mental illness (PMIs), and the elderly. All of these groups are more likely to be victimised through the use of technology including social media, emails, websites, and cell phones. Teenagers have been bombarded with social media and websites to the point of desensitisation, but they have rarely been taught how to distinguish factual and appropriate resources from the fraudulent. Teenagers are often targeted for non-monetary offences such as sex crimes. For PMIs and the elderly, cognitive decline and mental instability directly impact their level of scam awareness and decision-making. Many of these individuals have easy access to money. During the pandemic, they were worried about becoming infected and dying from COVID-19. Fear is a type of emotional arousal and is a common factor that enhances the effectiveness of all scams including COVID-19 online scams. And, technology makes it easy. At the height of the pandemic, websites promoted guaranteed test kits, vaccines, and cures. Scammers also used other electronic methods such as text messages, mobile phone calls, and emails. Some cybercriminals reportedly made personal home visits to victims to ensure the success of their scams. Part 2 presents several of these cases with a discussion of why the scams were so effective. Prevention tactics and education are emphasised, including a few programmes created to combat cybercrime and the appropriate people and agencies to contact for assistance. Finally, some guidance is provided on important steps that the public can take to help prevent their own exploitation and the victimisation of their family members.



PART ONE

COGNITIVE VULNERABILITIES LEADING TO SCAM SUSCEPTIBILITY AND VICTIMISATION

Online scams are rampant throughout the world. Cyber threats are always increasing (Neo, 2020). No one is safe. Humans have been identified as the most vulnerable component of the digital technology environment. Consequently, criminals target some specific demographics which include people who are most cognitively vulnerable (Acierno et al., 2010; Bonner & Johnson, 2018). These individuals include teenagers, the elderly, and persons with a mental illness (PMI). The proliferation of online technology and satellite communications has provided an easy tool for thieves through digital

accessibility and anonymity (Department of Justice [DOJ], 2021; TRIP, 2018). Cybercriminals will take full advantage of every weakness for their nefarious exploits. However, there is hope. Education, training, assessments, and awareness have the potential to reduce the effectiveness of cybercrimes.

Targetting the Vulnerable in a Time of COVID

The COVID-19 virus spread much more than just a physical illness across the planet. The virus spread fear. Basic necessities were in short supply in many

regions. People were required, or chose, to stay inside their homes to reduce the rate of infections and the spread of the disease. Social interactions between people almost became a crime. To this day in 2022, it is recommended that individuals continue to maintain their distance from others. The recommended distance is 6 feet which precludes touching others. This guideline interferes with human touch which is an excellent tool for reducing fear, stress, and loneliness (Eckstein et al., 2020). To help inhibit the spread of the virus, touching and congregating were not allowed. Psychological disorders increased and the virus still spread (World Health Organization, 2022). Many people tried to use digital technology like Zoom, Teams, and Facetime to connect with family and friends. In addition, many people began or increased their ordering and purchasing from online sources. All of this was intended to reduce the impact of COVID-19, but another unintended consequence occurred. The stage was set for a vulnerable world to become a very lucrative feeding ground for cybercriminals.

During the height of the pandemic, many people were desperate for the COVID-19 vaccine or a cure. People would scour the internet in search of an affordable or attainable solution. As a result, a multitude of fake vaccines and phony cures were offered on websites, television ads, email solicitations, and even by text messages (Federal Communications Commission, 2021). The cost of these bogus remedies was much more than money: People could lose their lives because they used these sham products instead of the real and legitimate ones. In addition, if they invested time, energy, and money on these scams, they would be delayed in obtaining the real vaccines and treatments that could save their lives (Bonner & Johnson, 2021).

One Swiss publication (Nolte et al., 2021a) documented a surge in fraudulent scams at the same time as the COVID-19 health impact was unfolding. In Singapore, there was a 163% increase in online scams at the beginning of the pandemic (Bose, 2021). Similar occurrences were also documented by the United States Federal Trade Commission (2020).

In the United States, the elderly are most victimised through identity theft fraud which is most easily perpetrated online (Federal Bureau of Investigation [FBI], 2021). Transnationally, the most common

elder fraud is romance scams followed by government imposter scams (DOJ, 2022). The common theme to these transnational schemes is that they occur through digital online methods. The criminals never meet with their victims. These common fraud scenarios are discussed more fully in Part 2 of this article.

Financially, the elderly document more monetary losses than younger age groups (Payne, 2020). In part, this is attributed to the fact that older individuals typically have more money than younger generations. While teenagers may be very susceptible to peer pressures, intimidation, and social media influences, they are unlikely to have the financial resources of the aged. As a result, the elderly are a very attractive target for cybercriminals (Reams, 2016; World Health Organization, 2018).

This background provides a foundation for the importance of cybercrimes in relation to vulnerable people such as the elderly. Criminals target the elderly more than any other group (Reams, 2016). Because of this targeting, the remainder of this article will concentrate on the elderly as a vulnerable population, some of the reasons that they are attractive targets, and several important psychological findings which may impede future victimisation.

Psychological and Cognitive Vulnerabilities: Ageing, Fear & Loneliness

Neurologically, the brains of children and teenagers have not fully developed (Phillips & Sternthal, 1977). They cannot analyse information and determine if it is accurate as well as adults can. They tend to be more trusting and accepting. They need education, experiences, and time to develop and strengthen neurological brain pathways. However, they do not have as much money as older adults, so they are not targeted as often with online scams as other vulnerable groups (Reams, 2016). In the online environment, teenagers and children are targeted more for sexual crimes.

PMIs and the elderly may be affected by cognitive decline and mental instability (World Health Organization, 2018). These problems will directly affect scam awareness and decision-making. In addition, with age, individuals become more likely to be diagnosed with a psychological disorder

(Haq, Edwards, & Thomas, 2019). Depression, anxiety, and insomnia are common in the elderly population. Therefore, there may be a certain level of overlap between some older adults and PMIs. Many psychological disorders affect cognitive functioning, providing a direct link to scam susceptibility. These disorders as well as others can make it difficult for older adults to make wise decisions, including financial decisions. Because of ageing and/or medications, both groups may demonstrate neurological deficits which make them more susceptible to cyberscams and victimisation.

As the brain ages, there is a direct impact on memory and cognition (Halber, 2018; Phillips & Sternthal, 1977; Yamaguchi et al., 2019). Short-term memories do not encode as well with age. Cognitive processing speeds become slower with age (Boyle et al., 2019). Therefore, it takes longer for the elderly to process information and they remember less of that information. These deficits make them more vulnerable to the deception and manipulation of scams. The elderly are more susceptible to repeated ads (by email, website pop-up, or text) especially if they are made by familiar celebrities from the past. Advertisers, unscrupulous businesses, and criminals will take advantage of these unfortunate circumstances (Reams, 2016).

Areas of the brain decline at different rates (Halber, 2018; WHO, 2018; Yamaguchi et al., 2019). The prefrontal cortex is the area dedicated to wise decision-making. Unfortunately, this is the area that declines earlier and faster than other brain areas. As the prefrontal cortex declines, the amygdala begins exerting more control. The amygdala is tasked with life-sustaining functions and emotions, including fear. With age, the brain relies more heavily on the emotion-focused centre instead of the logic-focused centre. This action increases the power of fear to affect behaviour and decisions. Cybercriminals take full advantage of fear and anxiety to persuade and deceive their victims. With the COVID-19 pandemic, all ages experienced an abundance of fear and anxiety which enhanced the effectiveness of the cyberscams.

Lu et al. (2020) studied the impact of emotional arousal on scam susceptibility. They used scam prevention posters that focused on normalising emotions and those that focused on rational cognitive messages. They found better resistance

to scams when the emotion-focused posters were used instead of the logic-focused posters. During this study, they also found that general emotional arousal, as measured by heartrate changes and self-reports, was not found to have an impact on scam susceptibility rates. This study was exploratory; so, further studies with different ages, cognitive abilities, and types of emotional arousal is warranted.

Yamaguchi et al. (2019) were interested in gullibility and Alzheimer's Dementia from the perspective of Theory of Mind (ToM). In this context, ToM is a cognitive process and refers to the ability to ascribe mental states to oneself and others. ToM is essential for good social interactions and to identify deception. The researchers were able to document that good ToM reasoning helped to reduce gullibility. They found a negative correlation: As cognition and ToM decrease, susceptibility to deception increases. For the elderly, it is much easier to interpret explicit and verbal communications than implicit and nonverbal communications. They also noted that with Alzheimer's Dementia, individuals have a specific difficulty in detecting insincere speech such as sarcasm, lies, and deception. These factors continue to provide an advantage for cybercriminals and a disadvantage for the targeted victims.

Lichtenberg, Stickney, and Paulson (2013) studied fraud and the possible relationship of psychological vulnerability in elderly individuals. Based on their research, they found that financial fraud attempts were more successful with those who were depressed and had insufficient social interactions. Fast forward to 2022 and Ueno et al. documented that limited social interactions were a risk factor for fraud susceptibility in elderly women in Japan. Hence, loneliness and isolation exacerbate the susceptibility of these individuals to scams. As can be identified in the transnational fraud data (DOJ, 2022), romance scams are the leading scam and they capitalise on the vulnerability of loneliness.

Experience Vulnerability: Past behaviour as predictor of future behaviour

One common risk factor for scam susceptibility is prior experience. Many studies have identified previous scam victimisation as an important risk factor for future victimisation (e.g., Campbell & Lichtenberg, 2020; Nolte et al., 2021b). Of

particular interest, Nolte et al. (2021b) conducted a study on willingness to contact scammers after reading an online solicitation letter. They documented that 75% of their 701 participants “realised the letter represented a scam but 43% were willing to respond”. This result begs for further psychological research.

Nolte et al. (2021b) emphasised that their study results were in the opposite direction of theorised reinforcement model results. Simplistically, if someone tries a risky online activity such as clicking on a questionable activation code, and nothing good happens, then that person is unlikely to repeat that action in the future. However, the obtained research results documented the opposite positive correlation: Previous risky online actions predicted risky online actions in this study. One study limitation was that the results of the previous risky actions were unknown. But, because they were scams, the expected results of the previous risky actions were assumed to have been negative or neutral at best (i.e., lost money or did not lose money but definitely did not obtain money).

The research results that Nolte et al. (2021b) obtained may be another justification of the old tenet in psychology: Past behaviour is the best predictor of future behaviour. Specifically, if the participants clicked once on a risky link, they would click again in the future. If they did not click initially, then they would be less likely to click in the future. Reinforcement theory would suggest that if they performed the risky action of clicking and received no good result then they would not perform the risky action of clicking in the future (because they received no good result). If they received a good result after the risky action, then more clicking would be expected in the future because the result is the determining factor and not the risk itself. Classic reinforcement theory emphasises the results of the behaviour (good or not good) instead of the behaviour itself (past risky clicking predicts future risky clicking). The study by Nolte et al. appears to support the pattern of risky behaviour instead of the results of the risky behaviour.

Furthering this analysis of applying reinforcement theory: To change the pattern of risky clicking, a specific result would have to occur. A positive

outcome (obtaining the promised money) should equate to an increase in risky clicking. A negative outcome (not obtaining the promised money) should produce a reduction in risky clicking. If money was taken (i.e., stolen), then an even greater reduction in risky clicking should occur. Classic Reinforcement Theory would propose that if money was stolen, the risky clicking should be extinguished. In reality, it appears that Nolte et al. (2021b) obtained the opposite result to classic models. These results may help explain the continued risky online behaviours of many people. Or, perhaps the wrong model is being used. Most people make a multitude of clicks while online and only a miniscule fraction may be harmful. Even with the harmful ones that might install a virus or trojan on the computer, most casual consumers of the internet are unaware that it has happened for a long time. Consequently, many users of technology may be lulled into complacency believing that most clicks online are safe. They may also believe that nothing bad will happen to them even if they click on something that is risky. (Please see the discussion in the next section of the research by Ueno et al. [2022] which illustrates this point.) Obviously, these theories regarding psychological models need objective and scientific research.

Another salient finding is in contrast to the idea that older adults are more vulnerable. Nolte et al. (2021a) found that the older adults exhibited slightly less susceptibility to COVID-19 scams. They postulated that this result may be due to older adults in this study considering the benefits to be lower and the risks higher in relation to COVID-19 promotions. The researchers suggested that impulse control and past scam experience might be the important factors in the scam susceptibilities that were identified.

Identifying Vulnerability Through Assessments

For their study, Boyle et al. (2019) developed a calculated scam score. In actuality, they were more focused on Alzheimer’s Disease than on the scams themselves. The researchers found that one unit increase in the calculated scam score (which represented lower awareness) resulted in a 60% increase in the risk of developing Alzheimer’s Dementia. As with most diseases, the earlier the identification, the sooner the disease-modifying therapies can be started.

The researchers emphasised that this study was only the beginning, but the results were promising. They requested further research into the development and validation of an objective and scientific Scam Awareness Measure. They reasoned that this measure may be a good component of an overall Risk Index and have good clinical utility for Alzheimer's Disease and Mild Cognitive Impairment. Besides the potential of a new diagnostic tool, this measure may provide awareness of an individual's need for education in scam awareness and gullibility.

In 2020, Campbell and Lichtenberg sought to create a short form (SF) of the Financial Exploitation Vulnerability Scale (FEVS). Through their research, they were able to identify an FEVS-SF with good psychometric properties and practical utility (see Figure 1). The results documented that the FEVS-SF was a better predictor than previously utilised demographic characteristics, risk factors, or cognitive abilities and was relatively equal to specific measures of executive functioning. The FEVS-SF consists of 9 items and is a good supplemental assessment for professionals who work with the elderly. The authors suggested that Adult Protective Services can use the scale quickly and easily. They

also promoted the FEVS-SF as providing actionable information related to standard of care.

In studying vulnerability from a different angle, researchers from Australia questioned whether there was a difference between gullibility and trust (Teunisse et al., 2020). With their research focus, gullibility was defined as "acceptance of a false premise". They conducted multiple studies to develop and evaluate a Gullibility Scale (GS; see Figure 2). Many of the situational cues in the studies were related to cybercrime such as online offers from a Prince to give the participant money. The researchers concluded that gullibility is a distinct construct. They also found a negative relationship between gullibility and social intelligence: As gullibility increases, social intelligence decreases, and vice versa. Overall, the GS was found to have sufficient psychometric properties providing some preliminary evidence that gullibility may be an enduring personality trait. With this in mind, further research with the GS may help identify "why some individuals are more likely than others to succumb to others' persuasion or manipulation".

For specific scam research, Yu et al. (2021) leveraged the ongoing Minority Aging Research

Figure 1. Campbell and Lichtenberg's questions for the Financial Exploitation Vulnerability Scale short form

- Overall, how satisfied are you with your finances?
- How often do your monthly expenses exceed your regular monthly income?
- How worried are you about having enough money to pay for things?
- How often do you feel downhearted or blue about your financial situation or decisions?
- How often do you feel anxious about your financial decisions and/or transactions?
- How often do you wish you had someone to talk to about financial decisions, transactions, or plans?
- How often do you worry about financial decisions you've recently made?
- How satisfied are you with this (money management) arrangement?
- How confident are you in making big financial decisions? Have you noticed any money taken from your bank account without your permission?
- Has a relationship with a family member or friend become strained due to finances as you have gotten older?
- How often do you talk with or visit others on a regular basis?
- How likely is it that anyone now wants to take or use your money without your permission?
- Who manages your money day to day?
- Are your memory, thinking skills, or ability to reason with regard to financial decisions or financial transactions worse than a year ago?
- Do you have a confidante with whom you can discuss anything, including your financial situations and decisions?
- Did anyone ever tell you that someone else you know wants to take your money?

Figure 2. Teunisse et al's Gullibility Scale

Composed of two factors, Persuadability and Insensitivity to Untrustworthiness Cues, you can test yourself on this measure by rating yourself on each of the following statements on a 1 (strongly disagree) to 7 (strongly agree) scale:

1. I'm pretty good at working out when someone is trying to fool me.
2. I'm usually quick to notice when someone is trying to cheat me.
3. I'm pretty poor at working out if someone is tricking me.
4. I quickly realize when someone is pulling my leg.
5. It usually takes me a while to "catch on" when someone is deceiving me.
6. I'm not that good at reading the signs that someone is trying to manipulate me.
7. My family thinks I am an easy target for scammers.
8. If anyone is likely to fall for a scam, it's me.
9. My friends think I'm easily fooled.
10. Overall, I'm pretty easily manipulated.
11. People think I'm a little naïve.
12. I guess I am more gullible than the average person.

Adapted by Susan Krauss Whitbourne, A New Way to Test Just How Gullible You Really Are, Psychology Today, March 7, 2020.

Study of the Rush Memory and Aging Project for specific scam research. The researchers made the case that many studies had been conducted on scams and their victims but these studies utilised predominately white participants. To address this limitation, Yu's team focused on elderly black individuals from the communities in and around Chicago in the United States. In this study, they utilised a 5-item scam scale. As expected, they found a negative correlation between impaired cognitive functioning and scam susceptibility (i.e., as cognitive functioning goes down, scam susceptibility goes up). Within cognition, semantic memory was a key factor in these results. They also found poor psychosocial factors and poor economic literacy correlated with increased scam susceptibility. Somewhat surprisingly, no difference was found with the characteristics of gender, physical health, educational level, or income level. Another notable difference was identified: Black elders were found to be less susceptible to scams than White elders. The researchers also postulated that many older Black adults may be strongly affected by the lack of self-determination which would have an important impact on scam susceptibility. The authors warned that many research parameters were different and further study should be conducted among elderly racial groups.

In 2022 in Japan, Ueno et al., conducted a research study with an emphasis on scammers trying to

impersonate family and friends of older individuals. This family impersonation scam is one of the top ten transnational cybercrimes (DOJ, 2022). Many factors were measured in this study and it included the authors' Scam Vulnerability Scale (SVS). Based on the scale, greater victimisation was identified by higher scores on both the item "I am confident that I will not be victimised by fraud" and on the item which supported listening to someone who comes to visit even if this person is unknown. Additional factors included being female, fewer excursions outside of home, and a lower educational level. This study was small but does reinforce concerns regarding loneliness and isolation and suggests value in considering these factors when trying to assess scam vulnerability in the elderly.

Psychological Impact of Victimisation

The consequences of cybercrime can be devastating. Money is not the only loss that elders suffer when they have been financially victimised. One common effect is feeling shame and guilt (DOJ, 2022; Haq, Edwards, & Thomas, 2019). Many victims feel angry. Often, elderly victims begin to doubt themselves. The elderly and other victim groups may develop or exacerbate psychological disorders such as depression and anxiety. Many times, elderly victims will not want to report the victimisation to family or authorities because they are embarrassed, or they worry that they might lose their freedom to live on their own.

Figure 3. Ueno et al.'s Scam Vulnerability Scale

The following statements are designed to measure susceptibility to fraud, which can be answered by older adults with cognitive decline.

- I am confident that I will not be scammed.
- If someone I do not know visits, I do not listen to them. (reverse item).
- Even if I am dissatisfied with my situation, I am overpowered by my opponent.
- I pick up the phone as soon as I get a call.
- I am interested in tempting offers.
- Even if I think the other person's story is suspicious, I think in a good direction.
- If someone I do not know talks to me in a strong tone, I will be frightened.
- If someone praises or gives special treatment to me, I will be happy.
- I feel anxious about talking to my family and friends about money because it is likely to lead to me losing their trust.

To truly address the breadth of the impact of victimisation on the elderly, PMIs, and teens, a multidisciplinary team with members from several professions is the best option (Haq, Edwards, & Thomas, 2019). Important team members include mental health professionals such as psychologists and social workers. The team should also include physicians and attorneys. Obviously, law enforcement professionals, adult protective services, or juvenile specialists must be the cornerstone of the team.

Summary

Overall, these studies provide evidence of a sincere desire to find the major factors in fraud victimisation as well as the impact of psychological and cognitive vulnerabilities. Humans have been identified as the weakest link in the cybercrime environment. The greater the number of relevant human factors that can be identified, the greater the potential to develop beneficial prevention tools and techniques.



PART TWO

CASE ILLUSTRATIONS, PREVENTION, MITIGATION, AND FUTURE DIRECTIONS

Cybercriminals employ many schemes to victimise citizens. As online shopping increases in popularity, alert notifications via the internet or cell phones have increased. Many appear as legitimate organisations or businesses with life-saving products. These cybercriminals have portrayed themselves as life-saving medical organisations or government agencies. They commit these false representations to gain personal information from victims. After obtaining data, cybercriminals use insurance information which provides them with a victim's identity to access other funds. Funds can include tax returns or stimulus money (Federal Trade Commission [FTC], 2022). Cybercriminals have

impersonated contract tracing employees to steal and use personal information from victims and their family members to commit thefts. The most reported scam to the FTC in 2020 was impersonator crimes and led to nearly 500,000 reports with a median loss of \$850 (FTC, 2021b).

Public education through government, law enforcement, and consumer protection agencies have done well to warn the public about cybercriminals. The public education includes scam techniques where imposters impersonate members of local charities to solicit funds. While these scams can be successful, little direct danger to the victim is usually present because the contact

methods involve disguised calls from outside of the victim's country. This is, however, changing. As one law enforcement expert put it, "Ten years ago, these scam calls were almost always made from outside the country. Today, not so much" (NW3C, 2022; DOJ, 2022). The return of the cybercriminal offering to come to a victim's home and take direct delivery of funds or obtain identity material is occurring with an alarming frequency. These contacts are often perpetrated upon victims who are homebound or have mobility issues.

These examples are only a small representation of the scam techniques outlined in this article.

Case Illustrations

In 2021, the FTC's annual Consumer Sentinel Network reported scammers were responsible for stealing approximately US\$86 million in 2020 due to scam texts. Further, the FTC reported US\$588 million in total losses for 2020 related to COVID scams. While trying to profit from the pandemic, these criminals sold **false cures and vaccines** that could cause sickness, death, or prevent a victim from obtaining legitimate medical treatment by providing false hopes they were immune or protected from COVID-19 (Food & Drug Administration [FDA], 2022).

Other scams and schemes were found to have a direct impact upon the health and welfare of the victims (FDA, 2022). The "Corona Destroyer Tea" was advertised as having the same benefits of an authorised COVID-19 vaccine but is made from the "all-natural" ingredients of a tea plant. One company marketed a product that claimed to be an "anti-COVID herbal inoculation" and was part of an "ongoing clinical research on effectiveness against COVID-19." Unproven products such as these were never evaluated by the FDA for safety and effectiveness related to the prevention or treatment of COVID-19 (FDA, 2022). These companies and many others were issued warning letters by the FDA and soon thereafter ceased to advertise or distribute their product.

Other scam examples provided by the FDA (2022) involved a Georgia (USA) subject who was selling misbranded drugs that were advertised and labelled as a treatment for COVID-19. This subject was arrested and later pled guilty. Similar to the

snake-oil salesman of days past in the American Old West, the suspect sold his "immunity shot" for \$19 a treatment and promised recipients they "could lower their risk of COVID-19 by 50% or more" (Warning Letters section). This criminal targeted victims who were aged 50 or above with this and other sales pitches on his company website.

Other websites promoting unlawful and unproven products used the following pitches to lure unsuspecting and worried victims into purchases:

- "The Next FIVE MINUTES could save your life"
- "This immune shot could be the most important formula in the WORLD right now due to the new pandemic"
- "Immune shot is not a Luxury, It is a Necessity RIGHT NOW"
- "Point Blank, If you Leave this site, You are at Risk"
- "Is Your Life Worth \$19? Seriously, Is It?" (FDA, 2022)

Many unproven products purporting to prevent or treat COVID-19, made from unknown substances under unknown conditions, present significant health risks in and of themselves. These false advertisements lead consumers to make choices that increase their risk of infection with COVID-19. Often these purchase decisions can convince citizens to delay or stop appropriate medical treatment (Centers for Disease Control and Prevention [CDC], 2021; FCC, 2021; FDA, 2021).

Cybercriminals are most successful while committing **impersonation scams** by obtaining personal information about their victims such as social security numbers or date of birth (Government and Information Services, 2021). One very common and successful way cybercriminals obtain information is through internet sources and social media. Victims who carelessly posted pictures of their vaccination card online with their personal information allowed scammers to impersonate them. By employing this tactic, scammers use this information to obtain COVID relief funds, tax returns, unemployment benefits and more (FTC, 2021a).

Another example of scams that negatively impact victims is centred around fake charities. The presence of **fake charities** is on the rise due to COVID-19 and the challenges associated with the pandemic. Every disaster or time of need highlights the pain

and suffering of persons directly affected by these tragedies. Charities, churches, and civic organisations offer services in an attempt to ease the suffering of those in need. Cybercriminals act just as quickly to take advantage of these events (FTC, 2021a). Citizens must be on the alert for organisations that want donations in cash, by gift card, or through money transfers. Payment methods such as these are nearly impossible to track and provide a layer of protection for the cybercriminals once they have the victim's funds. Individuals should only use credit cards or checks when donating. Citizens should keep records of all donations and review financial statements to verify only the charged amount a person agreed to donate is posted. Citizens should also make certain that recurring donations are not being made to a donor's account (FTC, 2021b).

Other common tactics for cybercriminals include coercing and intimidating victims into making decisions about donations in a hurried or rushed manner. Technology allows for scammers to edit or change caller identification systems to disguise calls and make them appear as if they are coming from local areas (FBI, 2021b). Scammers use similar and official names to mimic the names of real charities or organisations. Scammers claim that all donations are tax deductible to further confuse victims about the credibility of an organisation. Some scams advertise guaranteed sweepstake winnings in exchange for funds. These claims are also illegal (FTC, 2021b). These deductions are often not tax deductible.

Clean-up and debris removal related to storms or disasters is another common scam employed by scammers and cybercriminals. Scammers quote outrageous prices, demand payment up front, and often lack the ability or equipment to complete these services (DOJ, 2021). Citizens should not be pressured into employing these scammers even when legitimate contractors or service providers are unavailable. Citizens should ask for identification, business licenses, and proof of insurance. Final payment is only to be made when all work is completed and is satisfactory. Some victims are unable to live in their home due to storm damage and have to secure other accommodations. Sending funds or security deposits before meeting with prospective landlords or signing a lease often leads to tragic results due to scamming efforts (FTC, 2021b).

Business impersonator scams are on the rise as well. Cybercriminals claim to be employees of well-known companies and offer refunds for unauthorised purchases on a victim's account. This scam involves the cybercriminal "accidentally" transferring more funds than promised and asking the victim to send back the difference. Once the consumer makes this transfer, the scammer will then have access to move accounts and money among other accounts giving the appearance of a refund while moving funds to unrecoverable accounts (Senior Medical Patrol [SMP], 2021). Other versions of this scam include a call from a well-known company claiming that hackers have broken into the victim's account. The scammers insist the only way to protect their funds is to purchase gift cards and share the card number and PIN. Once this information has been passed along, there is no recovery of the funds or way to track the scammers (Department of Treasury, 2021).

Scams associated with social media ads offer assistance to sign up for U.S. government programmes that provide free phone and internet services. The victim is only required to provide money or personal information. The US government funds the Emergency Broadband Benefit Program, but it is completely free. Cybercriminals on the internet and by using social media deceptively use this programme to lure victims into providing personal information or money (FTC, 2021a).

Volunteers going door to door to provide information about COVID and vaccines exist in many communities. Citizens should never give personal information during these types of contact. Caution is urged to not respond to or open hyperlinks or text messages about COVID from unknown individuals (SMP, 2021). Contact tracers will never ask for Medicare numbers or other financial information. Further, contact tracers will not attempt to set up a COVID test which requires a payment (DOT, 2021).

COVID vaccination cards for sale are scams (Better Business Bureau, 2021). Personal information asked for during a phone contact related to COVID surveys are scams. Individuals should never provide personal information when offered money or gifts in exchange for taking the survey. Citizens need to be mindful of disposing of medical material such as syringes, vials, medicine bottles, records, or shipping packages. Scammers will resort to searching a person's trash

to obtain personal information (FBI, 2021a).

Medicare beneficiaries are often targets of unsolicited requests for updated personal, medical, or financial information. Medicare does not contact beneficiaries to offer services or reviews. Many unscrupulous medical labs have targeted retirement communities. These labs claim to be offering COVID tests while actually conducting lab tests and billing federal health care programmes for services that were medically unnecessary (Health & Human Services, 2021).

Some cybercriminals have even attempted to impersonate the chair of the FTC, the organisation tasked with investigating scammers. These cybercriminals will send emails that appear authentic and claim to provide access to COVID relief funds. All that is required is a reply with personal information such as name, address, and date of birth. Emails from unknown sources or unexpected senders that ask for a reply or directs a person to a link are **phishing scams** (FTC, 2021).

Robocalls identifying themselves as Medicaid representatives have been reported where victims are coerced to update their account to avoid late fees. The victims unknowingly provide their social security number to avoid being charged a late fee and having benefits interrupted. These calls are scams. Experts estimate that 75% of Medicare recipients in the United States are unfamiliar with how to replace a Medicare card (SMP, 2021). Cybercriminals take advantage of this knowledge gap and elicit vital information while pretending to procure new cards for victims.

Other **electronic scam** examples include the following:

- Text messages requesting driver license information in order to secure COVID funds. This occurred in the State of Florida, U.S. (Skiba, 2021).
- Phone calls from grandparents of military imposters claiming they are in trouble and need money fast for medical or travel expenses due to medical conditions (National Center on Elder Abuse, 2018).
- Emails or phone calls related to COVID funeral assistance to bury a loved one. Scammers search obituaries to contact surviving family members while claiming they are from the government and can provide burial assistance. The cybercriminals

claim they can easily enrol the family if the victims just provide personal information (Government Information & Services [GIS], 2021).

- Robocalls or texts from cybercriminals claiming they can provide early assistance checks from the Internal Revenue Service (IRS) by providing vital information. Another version of this scam includes fast checks ahead of everyone else for a small service fee. The cybercriminals utilise the victim's personal information to receive real cheques from the government by claiming to be the victim and the criminals keep all the funds (Department of Treasury [DOT], 2021).

These examples are common schemes that cybercriminals have used to take advantage of victims during the pandemic. Most of these schemes do not require a lot of money to start the process of taking victim's funds (FTC, 2021). Scamming and cybercrimes are often cheap and easy to employ. Protection and prevention does not have to be hard or complicated to implement. Many techniques exist for potential victims to use and avoid being the victim of fraud.

Prevention and Mitigation

The US Food & Drug Administration (FDA) has a dedicated COVID-19 Fraudulent Products Task Force that continues to monitor the market. This includes online monitoring to intercept fraudulent COVID-19 products. Operation Quack Hack employs agency expertise and advanced analytics to remove hundreds of unlawful products from the marketplace. As of June 2022, the agency has uncovered nearly 700 fraudulent products, sent more than 90 warning letters, issued more than 250 abuse complaints to domain registrars, and sent more than 150 requests to various marketplaces to remove listings for fraudulent COVID-19 products (FDA, 2022).

The US Federal Trade Commission (FTC) encourages all scams to be reported to government agencies. New scams are devised every day and authorities need this information to locate suspects, warn the public, and end fraudulent practices. Victims should not take for granted that the government is aware of all scam attempts. Citizens are urged to provide information, no matter how small or trivial. These pieces of information may be the key piece to apprehending scammers (FTC, 2021).

Charities should be researched before donations are made. In the United States, each state has a charity regulator. If a donor is unsure of a charity or has questions about its validity, charities can be investigated by going to the FTC website. Consumers can verify an organisation's authenticity through the Better Business Bureau (BBB) Wise Giving Alliance, Charity Navigator, and Charity Watch.

Cybercriminals can be convincing. If citizens or family members suspect a payment or donation to a scammer has occurred, they must act quickly (Bourne, 2000; FBI, 2021; Ministry of Health, 2022). As soon as possible, contact should be made with the bank, gift card, or credit card company utilised for the payment. The company must be informed of the fraudulent transaction. Requests to institutions for a reverse payment are encouraged to get funds returned. If a wire transfer is used through companies like Western Union or MoneyGram, the same procedures to request a reverse wire transfer to recover funds can be initiated. If cash is sent, recovery will be very difficult. Authorities urge notification to agencies such as the US Postal Inspection Service to intercept the cash. If another service is utilised, citizens should make contact and request assistance (FTC, 2021).

There are several additional tips that can aid in the prevention of scams. Some notable suggestions include the following:

- Never call back an unknown number.
- Based upon the request of an unknown person, citizens should not purchase and pay for anything with a gift card.
- Do not give remote access to computers or financial accounts to anyone who makes contact unexpectedly.
- A doctor or known medical professional should be the only person recommending or ordering tests or medical treatments related to COVID (SMP, 2021).
- Do not provide Medicare numbers to unknown sources. Unneeded or expensive services can be ordered by companies and scammers to capitalise on COVID related treatments (DOT, 2021).

The personal contact method by some scammers is on the increase. These personal contacts can be very dangerous and can lead to death or injury to the victim in their own home. However, for law enforcement and the informed citizen, these encounters present an opportunity to lure

cybercriminals into situations where they can be identified and brought to justice. Care and extreme caution should be exercised by the citizen and law enforcement to ensure the safety of the citizen during these encounters. Citizens should never initiate this type of contact without first consulting and working with law enforcement (DOJ, 2022).

Future Schemes of Cybercriminals

As the pandemic progresses, cybercriminals will try to devise the "what's next" scheme to stay ahead of enforcement actions and profit from their illegal activities (Brown et al., 2014; FTC, 2021). As of September 2022, 68% of the United States population has been fully vaccinated against COVID-19 (CDC, 2022). It has taken approximately 30 months to achieve that percentage of vaccinations. There is still plenty of time for crooks to scam the other 32% of the population. Vaccine scams are not expected to leave anytime soon. Booster shots are a likely target of COVID-19 mitigation. Scammers will try to exploit this treatment in a similar manner that was attempted with test kit availability at the beginning of the pandemic (GIS, 2021).

Test kits were in short supply or non-existent at the very beginning of the outbreak. Leaders around the world were faced with finding a reliable test kit along with creating a rapid test kit that could determine illness in a timely manner. In the weeks it took to develop these vital medical resources, scammers preyed on fears and uncertainty in a society that had not experienced a pandemic in over 100 years. When vaccines became available, test kit production was reduced. Demand for test kits have re-emerged due to vaccine resistance by large portions of the world. Some governments have regulations that require testing in lieu of vaccination. Scammers have reverted back to scams related to limited test kit availability to take advantage of the changing nature of COVID-19.

CONCLUSIONS

The COVID-19 pandemic is not over and may be with us for the near future. Vaccination rates are increasing and new challenges have occurred. Different surges have been experienced during these trying years (Skiba, 2021). Variants have occurred and can be expected to evolve over time. Political polarisation has been attributed to the vaccine and COVID treatment and can be expected to continue.

In totality, these different threats keep the anxiety high around the world. Cybercriminals will not stop in their efforts to capitalise on public mistrust, fear, and inaccurate information. And, scamming efforts are sure to continue around the world.

The importance of scam awareness is especially vital regarding the elderly. The elderly and their caregivers, families, and loved ones must know who to call, when to call, what to expect, and how they can help when reporting and fighting scammers (Brown et al., 2014; FBI, 2021b; FCC, 2021). It is important for all citizens to remember the following scam prevention techniques:

- Do not respond to calls or texts from unknown numbers or any others that appear suspicious.
- Never share personal or financial information via email, text, or over the phone. Governments and official agencies will never ask for this information using these methods and will never ask for money.
- Be extremely cautious if being pressured to share any information or make a payment immediately. Cybercriminals prey on the rapid infection time of COVID that makes the elderly gravely ill.
- Always check on charities that ask for help. The Better Business Bureau and state agencies maintain lists of legitimate charities.
- Contact law enforcement authorities immediately if there is any question that a citizen has been

the victim of a scam. Complaints can also be filed online with the FTC and various government resources (FTC, 2021a).

Following these scam prevention techniques can help protect all citizens, their financial security, and their way of life. Cybercriminals have the potential to be dangerous criminals. Many citizens in our society are fearful and can be preyed upon. COVID-19 has only provided a new avenue for cybercriminals to fraudulently steal from honest, unsuspecting individuals. With the help of government resources, knowledge of the problem area, and vigilance, all citizens may be protected from the treacherous efforts of scammers during uncertain times.

This article was adapted and supplemented from the following:

- Bonner, M., & Johnson, M. (2022). The effectiveness of cybercriminals with COVID-19 online scams: Part 1 – Cognitive Vulnerabilities. Presented at the 5th Asian Conference of Criminal and Operations Psychology (ACCOP), Singapore. Virtual.
- Johnson, M., & Bonner, M. (2022). The effectiveness of cybercriminals with COVID-19 online scams: Part 2 – Case Illustrations, Prevention, & Future Directions. Presented at the 5th Asian Conference of Criminal and Operations Psychology (ACCOP), Singapore. Virtual.

ABOUT THE AUTHORS



McKay Bonner

is a Licensed Psychologist and Full Professor in the Criminal Justice & Psychology Departments at the University of Louisiana Monroe (ULM). She teaches many courses including Criminal Behaviour, Forensic Psychology, Psychological Assessment, and Research Methods. Dr. Bonner has been the Public Safety Psychologist for several police, sheriff, and fire departments for over 20 years conducting evaluations for hiring, fitness, and officer-involved shootings. She is a law enforcement trainer at the Regional Police Academy and the Co-Coordinator for the Northeast Delta Crisis Intervention Team. She is a National Instructor and Facilitator for Active Bystandership for Law Enforcement (ABLE). She has worked with personnel throughout Louisiana, the United States, and Canada. Dr. Bonner has co-authored many articles, book chapters, and conference presentations. She is a member of the Society for Police and Criminal Psychology, and a reviewer for the *Journal for Police and Criminal Psychology* and *Police Practice and Research: An International Journal*. In 2020, she received the Louisiana Psychological Association 2020 Psychology in the Public Interest Award and the Psychology Times Community Innovation Award. She has a B.A. and M.S. from ULM and a Ph.D. from the University of Southern Mississippi.



Mark S. Johnson

is an Assistant Professor in Criminal Justice at the University of Louisiana Monroe (ULM) teaching Policing, Criminal Investigations, Industrial & Business Security, and Management of CJ Agencies. He retired with 30+ years of law enforcement experience with the Los Angeles County Sheriff's Department, U.S. Army-Military Police, Monroe Police Department, and ULM Police Department. His career includes extensive experience in training, narcotics, investigations, special operations, event coordination and security, corrections, public information, and Crimestoppers and ended at Assistant Chief. He is a POST Certified Police Academy Instructor in traffic stops, firearms, use of force, special operations and tactics, homicide/robbery investigations, and EVOG. He has been qualified and testified as an expert witness in state and federal courts. He is the Co-Coordinator for the Northeast Delta Crisis Intervention Team. Previously, he served on the Louisiana Governor's Task Force for Vehicular Homicide and Driving While Intoxicated enforcement. He is a past president of the Municipal Police Officers Association and the Louisiana Peace Officers Association. Dr. Johnson has co-authored journal articles and book chapters and presented at the professional conferences of the Society for Police and Criminal Psychology. He has a B.A., M.A., and an Ed.D. from ULM.

REFERENCES

- Acierno, R., Hernandez, M., Amstadter, A., Resnick, H., Steve, K., Muzzy, W., & Kilpatrick, D. (2010). Prevalence and correlates of emotional, physical, sexual, and financial abuse and potential neglect in the United States: The national elder mistreatment study. *American Journal of Public Health, 100*(2), 292-297.
- Alzheimer's Association. (2018). 2018 Alzheimer's Disease facts and figures. *Alzheimer's Dementia, 14*(3), 367-429.
- Better Business Bureau. (2021). *Scam Tracker*. Retrieved August 23, 2021 from www.bbb.org/scamtracker
- Bonner, M., & Johnson, M. (2013). The intersection between law enforcement and persons with a mental illness. *Crime, Punishment, and the Law, 3*(1), pp. 15-26.
- Bonner, M., & Johnson, M. (2018). Encounters between the elderly and law enforcement: An overview of mental illness, addictions, victims, and criminals. *Contemporary Southern Psychology (renamed Multidisciplinary Psychology: A Journal of Collaboration)*, Vol 1. Reprinted 2022 Vol 2(2).
- Bonner, M., & Johnson, M. (2021). COVID-19 medication scams, cognitive decline, & the elderly. Presented at the Psychology and Aging Resource Collaborative's 2021 (PARC) Addiction and the Elderly III Symposium, Monroe, LA.
- Bose, S. (2021). COVID-19: The evolution of scams in Asia-Pacific. *Information Technology*, Singapore.
- Boyle, P., Yu, L., Schneider, J., Wilson, R., & Bennet, D. (2019). *Scam Awareness Related to Incident Alzheimer Dementia and Mild Cognitive Impairment*. *Annals of Internal Medicine*. Retrieved August 19, 2021 from <https://doi.org/10.7326/M18-2711>
- Bourns, W. (2000). Police gerontology services for the elderly: A policy guide. *Justice Professional, 13*(2), 179-193.
- Brown, R., Ahalt, C., Steinman, M., Kruger, K., & Williams, B. (2014). Police on the front line of community geriatric health care: Challenges and opportunities. *Journal of the American Geriatrics Society, 62*(11), 2191-2198.
- Campbell, R., & Lichtenberg, P. (2020). A short form of the financial exploitation vulnerability scale. *Clinical Gerontologist: The Journal of Aging and Mental Health*. <http://dx.doi.org.ulm.idm.oclc.org/10.1080/07317115.2020.1836108>
- Centers for Disease Control and Prevention. (2022). *Covid-19*. <https://www.cdc.gov/coronavirus/2019-ncov/index.html>

- Cordner, G. (2006). *People with a mental illness*. Community Oriented Policing Services; Problem-Oriented Guides for Police. The U.S. Department of Justice.
- Department of Justice. (2021). *Fraud Related to COVID-19 Virus (Coronavirus)*. <https://www.justice.gov/disaster-fraud>
- Department of Justice. (2022). Responding to Transnational Elder Fraud. *National White Collar Crime Center*. <https://www.nw3c.org/>
- Department of the Treasury. (2021). *Covid-19 Scams*. <https://home.treasury.gov/services/report-fraud-waste-and-abuse/covid-19-scams>
- Eckstein, M., Mamaev, I., Ditzen, B., & Sailer, U. (2020). Calming effects of touch in human, animal, and robotic interaction – Scientific state of the art and technical advances. *Frontiers in Psychology, Social Neuroscience*. <https://doi.org/10.3389/fpsy.2020.555058>
- Federal Bureau of Investigation (2021a). 2020 IC3 Elderly Fraud Report. https://www.ic3.gov/Media/PDF/AnnualReport/2020_IC3ElderFraudReport.pdf
- Federal Bureau of Investigation (2021b). *FBI Urges vigilance during COVID-19 Pandemic*. <https://www.fbi.gov/coronavirus>
- Federal Communications Commission. (2021, August 26). *Corona Virus Scams – Consumer Resources*. <https://www.fcc.gov/covid-scams>
- Federal Trade Commission (2020). Data and visualizations. *United States Government*. <https://www.ftc.gov/enforcement/data-visualizations>.
- Federal Trade Commission. (2021a). *Consumer Sentinel Network*. <https://www.ftc.gov/enforcement/consumer-sentinel-network>
- Federal Trade Commission. (2021b). *Coronavirus (COVID-19) Pandemic: The FTC in Action*. <https://www.ftc.gov/coronavirus>
- Food and Drug Administration. (2022, September 23). *Fraudulent Coronavirus Disease 2019 (COVID-19) Products*. <https://www.fda.gov/consumers/health-fraud-scams/fraudulent-coronavirus-disease-2019-covid-19-products>
- Government Information and Services. (2021). *Covid-19*. <https://www.usa.gov/coronavirus>
- Halber, D. (2018). Adult and aging brain. In *Brain Facts: A primer on the brain and nervous system* (8th ed.), 53-58. Society for Neuroscience: Washington, D.C.
- Haq, A., Edwards, M., & Thomas, N. (2019). Financial abuse of the elderly: The role of psychiatrists: Session 415. *American Journal of Geriatric Psychiatry*, 27, Supplement, p S48-S48.
- Harrell, E. (2015, September). *Victims of Identity Theft, 2014*. Bureau of Justice Statistics Bulletin. U.S. Department of Justice. <https://bjs.ojp.gov/library/publications/victims-identity-theft-2014>.
- Health and Human Services. (2021). *Find ways to prevent, treat, or help fight COVID-19*. <https://combatcovid.hhs.gov/>
- Lichtenberg, P., Stickney, L., & Paulson, D. (2013). Is psychological vulnerability related to the experience of fraud in older adults? *Clinical Gerontologist*, 36(2), 132-146.
- Lu, H.Y., Chan, S., Chai, W., Lau, S.M., & Khader, M. (2020). Examining the influence of emotional arousal and scam preventive messaging on susceptibility to scams. *Crime Prevention and Community Safety*, 22(4).
- Ministry of Health, Singapore (2022). *What to do in case of Cyberattack?* <https://www.moh.gov.sg/licensing-and-regulation/cybersecurity>
- National Center on Elder Abuse. (2018). *NCEA and Covid-19*. U.S. Administration of Aging. <https://ncea.acl.gov/Resources/COVID-19.aspx>

- Neo, L. (2020). Leveraging on digital footprints to identify potential security threats: Insights from the behavioral sciences perspective. In M. Khosrow-Pour's (Ed.) *Encyclopedia of Criminal Activities and the Deep Web, Volume 3*.
- Newman, L. (2020). Watch out for coronavirus phishing cams. *Wired.com*. Available online at <https://www.wired.com/story/coronavirus-phishing-scams/>
- Nolte, J., Hanoch, Y., Wood, S., & Hengerer, D. (2021a). Susceptibility to COVID-19 scams: The roles of age, individual difference measures, and scam-related perceptions. *Frontiers in Psychology, 12*, pp 789883.
- Nolte, J., Hanoch, Y., Wood, S., & Reyna, V. (2021b). Compliance with mass marketing solicitation: The role of verbatim and gist processing. *Brain and Behavior, 11*(11).
- NW3C. (2022). *Responding to Transnational Elder Fraud*. <https://www.nw3c.org/>
- Payne, B. (2020). Criminals work from home during the pandemics too: A public health approach to respond to fraud and crimes against those 50 and above. *American Journal of Criminal Justice, 45*, 563-577.
- Phillips, L., & Sternthal, R. (1977). Age differences in information processing: A perspective on the aged consumer. *Journal of Marketing Research, 14*, 444.
- Reams, J. (2016). Twenty-First Century Advertising and the Plight of the Elderly Consumer, *Willamette Law Review, 325-352*, 05/31/2016.
- Senior Medical Patrol. (2021, August). *SMP Consumer Fraud Alert: COVID-19*. <https://www.smpresource.org/Content/Medicare-Fraud/SMP-Consumer-Fraud-Alerts/SMP-Consumer-Fraud-Alert-COVID-19.aspx>
- Schmitt, R. (2017, March 15). Elder abuse: When caregiving goes wrong. *AARP Bulletin*. American Association of Retired Persons. Retrieved from <https://www.aarp.org/caregiving/basics/info-2017/elder-abuse-assisted-living.html>
- Skiba, Katherine. (2021, February 24). *10 Red-Hot COVID Scams Vexing Older Americans*. AARP. <https://www.aarp.org/money/scams-fraud/info-2021/covid-19-scams-vexing-older-americans.html>
- Teunisse, A., Case, T., Fitness, J., & Sweller, N. (2020). I should have known better: Development of a self-report measure of gullibility. *Personality and Social Psychology Bulletin, 46*(3), pp 408-423.
- TRIP. (2018, March). Preserving the mobility and safety of older Americans. National Transportation Research Group. Washington, D.C. https://tripnet.org/wp-content/uploads/2019/07/Older_Americans_Mobility_TRIP_Report_2018.pdf
- Ueno, D., Arakawa, M., Fujii, Y., Amano, S., Kato, Y., Matsuoka, T., & Narumoto, J. (2022). *Psychosocial characteristics of victims of special fraud among Japanese older adults: A cross-sectional study using scam vulnerability scale*. *Frontier Psychology, Sec. Psychology of Aging*. doi: 10.3389/fpsyg.2022.960442
- World Health Organization. (2017). *Mental health of older adults*. Fact Sheet. The World Health Organization. Retrieved from <http://www.who.int/en/news-room/fact-sheets/detail/mental-health-of-older-adults>
- World Health Organization. (2018). *Mental health of older adults*. Fact Sheet. The World Health Organization. Retrieved from <http://www.who.int/en/news-room/fact-sheets/detail/mental-health-of-older-adults>
- World Health Organization. (2022). COVID-19 pandemic triggers 25% increase in prevalence of anxiety and depression worldwide. Retrieved from <https://www.who.int/news/item/02-03-2022-covid-19-pandemic-triggers-25-increase-in-prevalence-of-anxiety-and-depression-worldwide>
- Yamaguchi, T., Maki, Y., Takatama, M., & Yamaguchi, H. (2019). Gullibility may be a warning sign of Alzheimer's disease dementia, *International Psychogeriatrics, 31*:3, 363-370, International Psychogeriatric Association.
- Yu, L., et al., (2021). Correlates of susceptibility to scams in community-dwelling older black adults. *Gerontology, 67*: 729-739. <https://doi-org.ulm.idm.oclc.org/10.1159/000515326>

EXPLORING GUARDIAN-CENTRIC SCAM PREVENTION ATTITUDES: HELP! HOW DO I PROTECT MY LOVED ONE FROM JOB SCAMS?

Stephanie Chan & Amanda Tan

Home Team Psychology Division, Ministry of Home Affairs, Singapore

ABSTRACT

Guardians play a crucial role in building Singapore's societal resistance against scams by preventing their loved ones from falling prey to scammers. Apart from relaying information to their loved ones on recent scam trends and cautioning them against scam attempts, they also provide the much-needed social support to loved ones who are making emotionally driven decisions. Given the rise of scam cases in recent years, particularly job scams in Singapore, it has become increasingly important that the guardians are able to effectively advise their loved ones who encounter persuasive job scam messages. This study focuses on the persuasion techniques used in job scam scenarios and examines resistance strategies adopted by 133 guardians who participated in an immersive survey designed by the authors using mock vignettes culled from actual cases. Supported by our research findings, the study then recommends two strategies that can further equip guardians with information and support needed to provide effective advice to loved ones.

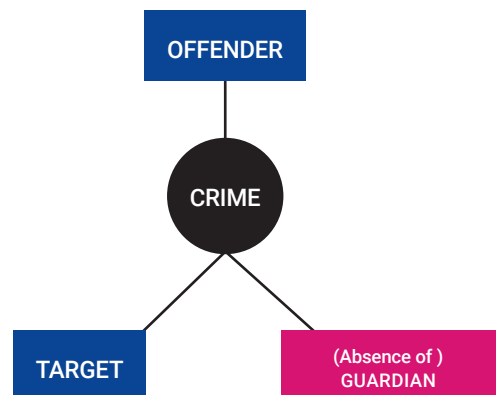
COMMUNITY GUARDIANS IN SINGAPORE'S FIGHT AGAINST SCAMS

Scams are dynamic and scammers are constantly adjusting their techniques to lure in targets. In recent years, Singapore has seen a rise in a particular scam type – job scams – with a total of 4,554 reported cases in 2021, up from only 132 reported cases in 2020 (Singapore Police Force, 2021). The worrying trend continues with 3,573 reported cases in the first half of 2022 (Singapore Police Force, 2022).

In the field of criminology, the Routine Activities Theory (Cohen & Felson, 1979) lays down three situational conditions for a successful crime to occur: a likely offender, a suitable target, and the absence of a capable guardian (see Figure 1). The third condition pertaining to the role of guardians and the impact of their absence and/or their incapability has lately drawn the attention of stakeholders in the fight against scams. Early research on traditional interpersonal and property crime has found support for the passive presence of guardians (Leclerc, Smallbone, & Wortley, 2013; van Sintemaartensdijk

et al., 2021) and stronger evidence for the active intervention of guardians to deter and disrupt an interaction between the offender and the target (Hollis-Peel, et al., 2011; Reynald, 2009; Sampson, Eck, & Dunham, 2010).

Figure 1. The three situational conditions of the Routine Activities Theory of Crime



Guardianship plays a critical role in Singapore's ongoing efforts in combatting scams. For would-be victims of scams (i.e., targets), they often turn to their family members, peers, or closest friends and colleagues for advice and support in their times of need. For guardians, by alerting loved ones to the latest scam trends or cautioning them against scam attempts, they informally serve as a "line of defence". The National Prevalence Survey on Scams in Singapore 2019-2020 likewise found that community guardians play an important role in building Singapore's societal resilience and resistance against scams (ScamAlert, 2020). Accordingly, Project PRAISE was launched in July 2022 by the Singapore Ministry of Home Affairs (MHA) to empower and educate the public to be wary of scams (Ministry of Home Affairs, 2022).

Standing for Police-RSVP Anti-Scam Engagement, PRAISE works by recruiting and training senior citizen volunteers to spread anti-scam messages amongst their peers (Lim, 2022). It has since made an impressive outreach to more than 526 senior citizens in the initial runs (Ministry of Home Affairs, 2022). This type of community advocacy is valuable because, as noted by Minister of State (Home Affairs) Sun Xueling, "seniors will be able to turn to those in the same age group and are more likely to trust them because they have been through similar lived experiences and have a similar level of understanding of digital devices" (Lim, 2022).

SCOPE AND PURPOSE OF STUDY

This paper explores the "Hows" and "Whys" in which community guardians, specifically family members and close friends, give anti-scam

advice to their loved ones who are encountering persuasive job scam messages. Given the rise in communications technologies, cybercrime goes beyond spatial and temporal boundaries and alters one's social interactions with others. This might result in unique challenges for community guardianship efforts to prevent scams. Yet, there is a dearth of local research or surveys on guardianship in this area of scams.

An immersive survey was designed to capture the attitudes and actions undertaken by 133 family members and close friends (i.e., community guardians) in dealing with various job scam scenarios. Mock vignettes were modelled after job scam variants reported by the Singapore Police Force in 2021 and self-reported by members of public on the ScamAlert website. Additional research was drawn from articles in professional journals on persuasion techniques and reactance behaviours, and from research reports written for the Home Team by the Home Team Behavioural Sciences Centre (HTBSC). The study findings, by highlighting the attitudes and needs of local community guardians, can then be used to affirm and enhance current anti-scam initiatives used by local private and public community partners.

Designing an Immersive Survey with the Persuasive Elements of Job Scams

It is extremely challenging when a loved one encounters a persuasive scammer. Many job scams utilise a deadly combination of elements of persuasion. Building on the research by Robert Cialdini (2021), local cases of job scams can be classified as containing a range of six types of persuasion techniques (see Figure 2).

Figure 2. Six types of persuasion techniques seen in local job scams in 2021.



Mock job scam vignettes in this study were designed to contain realistic elements of persuasion. Each vignette consisted of 2-3 parts of a storyline of which participants were encouraged to take on the role of advising their loved one who were facing such scenarios. The storylines were presented in a naturalistic manner, with each part containing one type of persuasion technique:

For each vignette, all participants responded to the same set of open-ended questions:

- What would you say to your loved one?
- What else would you do?
- Why would you advise in such a manner?
- How confident (scale of 1 to 5) are you in your advice?

Sample of Mock Vignette:

On a Thursday evening, you received a call from your cousin. He tells you that he was introduced to a job a few days ago by an unknown number claiming to be "John". John had instructed him to download an application and complete tasks by topping up his account via bank transfers.

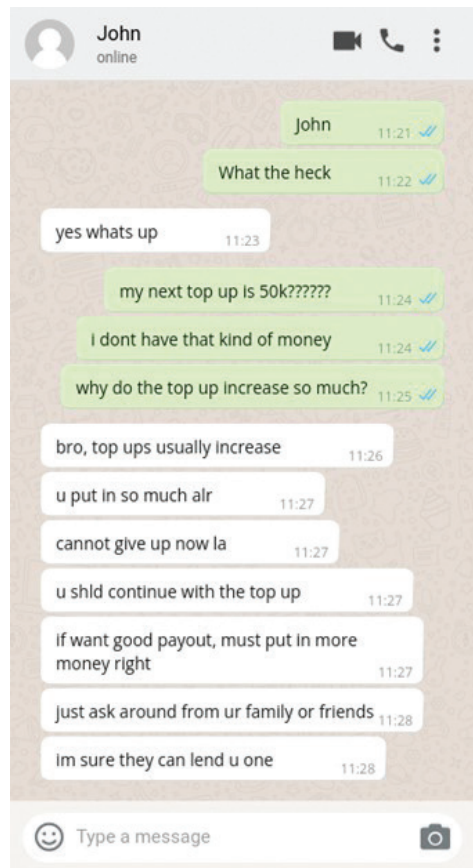
Your cousin says that he had initially done a top-up of \$5,000 and now needs to do a top-up of \$10,000. John offered to loan him \$5,000. Being unsure of what to do, your cousin sends you a screenshot of the conversation (see image on bottom).

Continuation of Mock Vignette:

The next day, you receive another call from the same cousin.

You realized that he had continued with the job and now needed to do a top-up of \$50,000. John had advised him to continue with the job.

Your cousin is not sure what he should do and sends you a screenshot of the conversation (see image on bottom).



This study employed three mock vignettes. Collectively, the vignettes contained the six persuasion techniques described by Cialdini (2021), viz.:

1. Reciprocity: People feel an obligation to give back to others (i.e., return the gesture) when they have first received something from them.
2. Scarcity: People tend to want more of the things that they think they cannot have (i.e., a form of loss aversion).
3. Authority: When in doubt, people tend to follow the lead of credible and knowledgeable “experts”.
4. Consistency: People tend to want to be consistent with their own previous actions or words.
5. Liking: People prefer to say “yes” to individuals that they like. This includes those who are similar to us, who praise us, who cooperate with us, and who seem to have mutual goals.
6. Social Proof: When feeling uncertain, people tend to look to the actions and behaviours of others to determine their own actions.

This survey was conducted online, and participants were obtained via purposeful “snowball” sampling via WhatsApp and other social media platforms based on their accessibility and availability. In view of the COVID-19 pandemic restrictions during the period of data collection, participant recruitment was not done face-to-face which may have affected the numbers for participation and/or survey completion. Nevertheless, the survey encouraged participation by highlighting the prevalence of scams and the importance of tackling scams (i.e., social motivation). Participation in the survey was voluntary and anonymous.¹

Rich qualitative data was captured based on 133 completed responses to the survey. All participants were aged 15 years and above, with a good spread across various age groups (i.e., mainly those in their 20s, 30s, 40s, and 50s).

A few of the respondents – 19 or 14% – had previously been victims of scams. About a third – 47 or 35% of respondents – had family, close friends or loved ones who previously fell prey to scammers.

Key Findings: How (And Why) Do Guardians Advise Loved Ones Who Encounter Job Scams?

The literature on resistance towards persuasion in varying contexts (e.g., advertisements, newsfeed, behavioural nudging messages) posits that individuals can have three types of reactance behaviours towards persuasion (Fransen et al., 2015):

- **Avoidance** is the most passive strategy comprising physical avoidance, cognitive avoidance, and mechanical avoidance (de Gregorio et al., 2017; Johnson, 2013). In an online communications context, this could mean refusing to respond to suspicious texts or refusing to click on a provided link.
- **Contesting** is an active source-facing strategy involving challenging the content, the source, or the persuasion tactic used (Albarracín & Karan, 2022; Friestad & Wright, 1994). This could mean doubting the validity of the individual/app/company or fact-checking the information/details provided.
- **(Self) Empowering** is an active inward-facing strategy comprising attitude bolstering, social validation, and self-assertion (Abelson, 1959; Zuwerink-Jacks & Cameron, 2003). This could mean “holding fast” to one’s existing attitudes or seeking the support of significant others to validate one’s existing attitudes.

This study began with the hypothesis that guardians of scams would display similar advice of avoidance, contesting, or empowering towards their loved ones who encountered persuasive job scams. The findings mainly confirmed the hypothesis but also revealed more nuanced approaches, as explained below.

¹ The survey methodology, questions, and mock job scam vignettes are available from the authors upon request.

#1: Guardians' Main Preference is to Advise Avoidance

It is important to note that many participants provided a combination of advice to the vignettes (see Figure 3). Still, the more frequent type of response was to advise loved ones to avoid the scammer – there were 340 mentions of avoidance methods mentioned by the participants, including deleting the text, blocking the number, asking the loved one to ignore the text, and adjusting phone privacy settings of loved ones. As the use of the avoidance strategy is the most passive form of resistance (Fransen et al., 2015), it is the most convenient way to resist being persuaded by job scam messages. For guardians, it is expected that they would retain behavioural consistency of their intentions (Cialdini, 2021) and convey the same avoidance type of advice to their loved ones who are encountering persuasive job scams. The National Prevalence Survey on Scams 2019-2020 likewise found that “near-misses” chose to evade scammers via avoidance means, such as not picking up calls from unknown phone numbers (ScamAlert, 2020).

As for other types of responses, “contesting”, being an active form of resistance (Albarracin & Karan, 2022), was less frequently used compared to avoidance, but still used quite commonly. There were 219 mentions of contesting methods cited by the participants, including voicing doubts on

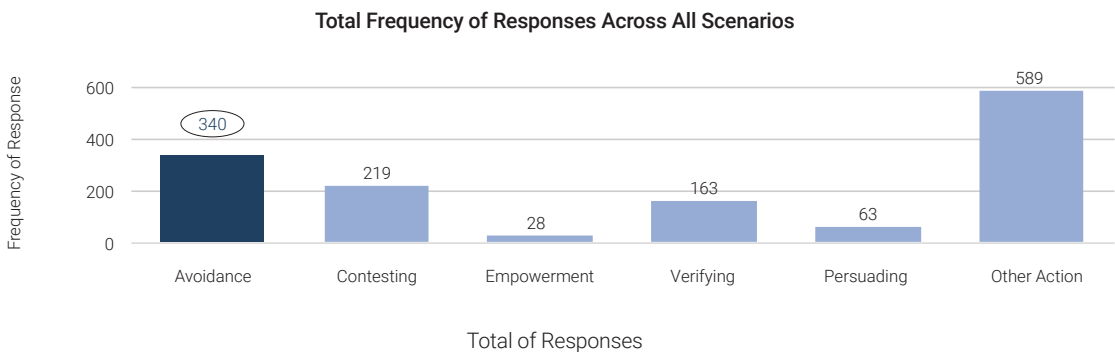
the authenticity of the job offer, suggesting that the texter was using a fake name, and pointing out persuasion techniques to the loved ones’ attention. As a contesting strategy requires more assertive action from the participants, this could be the reason that it was less used compared to an avoidance strategy.

The main difference between a contesting strategy and a verifying strategy is that for “verifying”, participants merely suggested to the loved ones to verify and seek the opinions of other family members or urged them to conduct fact-checking. Such verbal advice to loved ones did not result in the participants personally taking concrete action to combat the scam attempt. Nevertheless, this was an interesting form of response from the participants that is not seen in the literature. As qualitative data was not sought from participants in this survey regarding their rationale for choice of resistance strategies, future research could explore the nuances regarding scam guardians’ preferences and motivations for usage of resistance strategies.

#2: Guardians are Less Confident when Scammers Utilise “Liking” Persuasion

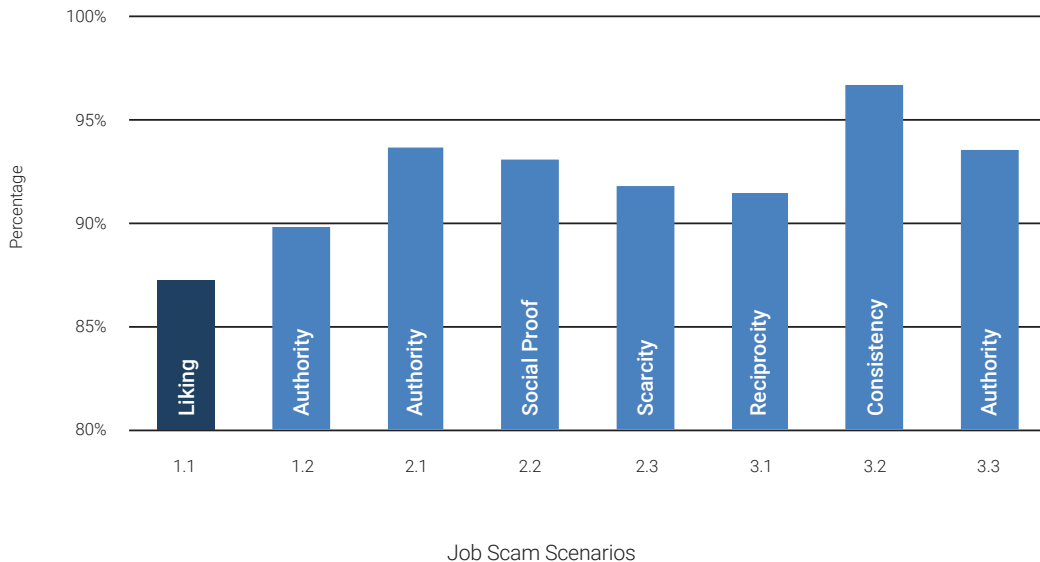
Guardians were asked to rate their confidence level pertaining to their given advice to their loved one (scale of 1 to 5). As each part of a vignette

Figure 3. Types of responses from guardians towards their loved ones.



Note: “Other Action” contains data referring to mentions of methods that did not categorise neatly, including offering financial support, assisting in collecting evidence, providing post-scam suggestions for recovery, or purely observational comments without specific advice given to the loved one.

Figure 4. Confidence levels in advising against different persuasion techniques.



contained one type of persuasion technique, guardians self-reported lowest confidence when providing advice to loved ones encountering job scammers who utilised the “liking” persuasion technique compared to other persuasion techniques (see Figure 4).

The persuasion technique of “liking” operates under the unspoken social rule that people prefer to say “yes” to individuals that they like (Cialdini, 2021). This may include scammers who claim to have similar interests as their victims or praise and cooperate with victims to reach supposedly mutual goals. The SIDE Theory (Social Identity Deindividuation Effects) argues that online communication features cause cyber users to have an “idealised perception” of others due to the absence of face-to-face cues and prior personal knowledge of the other party (Walther, 1996). In other words, impressions are formed based off minimal cues (Venter, 2019). This absence of opportunities for learned observations means that online users may choose to see the other party in a positive light and ignore conversational “red flags”. At present, such unique features of online communication may amplify the “liking” persuasion technique, posing challenges for community guardianship in the fight against scams. It is possible to interpret the findings

that guardians are aware of the challenges in convincing a loved one who trusts and likes a scammer who is claiming to be acting in the victim’s interest. As qualitative data was not sought from participants in this survey regarding elaboration on their self-reported confidence levels in advising loved ones, future research could investigate perceptions held by guardians towards combatting scams as considerations for policies in anti-scam prevention.

#3: Guardians Self-Reported Facing Challenges

Guardians were asked to provide their thoughts on the difficulties faced when providing advice to loved ones encountering job scammers. Overall, the respondents were aware of the impact of persuasive techniques on the mindset and motivations of their loved ones. Some of the verbatim responses obtained include:

“...don’t know for sure [if the job scenario is a scam], so might think there is no harm trying”

“They [loved one] will be reluctant to listen as the deals are too good”

“Their [loved ones] desperation ...for a job make them less receptive”

#4: Guardians Requested Support

Guardians generally understood their role in deterring and intervening in scams but expressed the need for informational support to enable them to play their role more effectively. Some of the verbatim suggestions obtained include:

"Real life cases reported on reliable news websites"

"How to provide helpful advice in a non-judgemental way"

FUTURE DIRECTIONS AND RECOMMENDATIONS FOR THE HOME TEAM

Empower Guardians

The role of guardianship in the fight against scams is undeniable. When loved ones have increased social support, it reduces the likelihood of them falling for scams (James et al., 2014). However, more must be done to ensure guardians are equipped to protect their loved ones. Findings from this survey show that guardians instinctively advise their loved ones to avoid scammers. Yet, **there are other ways of behavioural responses (e.g., contesting, empowering, etc.) which can expand guardians' repertoire of actions.** In fact, this survey suggests that many are willing to undertake these behavioural responses.

The current advisories provided to the public by the National Crime Prevention Council (NCPC), the Singapore Police Force, and other private enterprises include contesting strategies (e.g., "Ask yourself or others if this could be true", "Double confirm first", "Tips to identify a Lazada job scam"). Verbatim responses from several participants describe their willingness to challenge dubious sources/information/tactics but difficulties in distinguishing scams from genuine good deals. While further research is needed to ascertain if this is representative of the public's dilemma, there are indications that the scams landscape is dynamic, and scammers are constantly improving their methods. As such, **information needed to fact-check scams should be constantly updated** through a combination of law enforcement detection and community reporting efforts.

Additionally, **advisory examples should cover more examples of the persuasive elements**

used in scams. This enables quicker and more confident identification of persuasive tactics used by scammers. After all, guardians' ability to contest scams increase when they can verify the genuineness of a message/website/source.

Equip Guardians: Dealing with the Aftermath

According to the Singapore Counselling Centre (2022), victims often feel shame and helplessness after being scammed. This internalised shame can result in loss of self-esteem and social isolation. Often, victims choose not to share their struggles with others, negatively impacting their mental health and worsening their ability to cope and deal with the aftermath of a scam. This "downward spiral" and resistance towards seeking social help makes it challenging for guardians to step in and take up their role, even as communities grow to adopt a culture of mutual care and alertness. **Advisory platforms could be redesigned so that information needed to support loved ones emotionally is conveniently accessible to would-be guardians.** At present, information can be found in news articles (e.g., The Straits Times) or on well-known websites (e.g., ScamAlert) but the tips might not be "one click away". At best, such websites, through their wording and sentence phrasings, appear to be targeted towards victims for them to self-assist – guardians would have to assemble their own information or even translate the information into a different language to suit their loved ones' language preferences, which is a cognitively heavy task to carry out under stressful conditions.

CONCLUSION

Scammers often use a combination of persuasion strategies which are very effective in scamming victims. As such, guardianship is a highly encouraged "first line of defence" as part of community resilience. These protectors deter and intervene in scams by encouraging loved ones to avoid or contest scams, or even bolster the self-confidence of targeted victims to "hold fast" and not sway to the demands of scammers. At present, much more is needed to build guardianship efforts in Singapore given the perceived challenges encountered in supporting loved ones. Simple suggestions have been provided to show that contrary to belief, guardianship capability can be developed and maintained. It is hoped that this study, preliminary as it is, can kickstart efforts to strengthen the nation's defences against scams.

ABOUT THE AUTHORS



Stephanie Chan

is a Lead Psychologist with the Home Team Psychology Division. Stephanie's current research interest is in crime and forensic psychology, particularly in the law enforcement context. Her primary research area focuses on the psychology of detecting deception and deceptive intent, as this has operational applications for cyber detection and people profiling purposes.



Amanda Tan

was a research intern at the Centre for Advanced Psychological Sciences which has been incorporated into the newly formed Home Team Psychology Division at the Ministry of Home Affairs. Amanda's research interests include persuasion techniques in scams and deception tactics used by cybercriminals. Amanda is currently pursuing an undergraduate degree in Mathematics at the National University of Singapore.

The new **Home Team Psychology Division (HTPD)** was formed in the Ministry of Home Affairs on 1 February 2023, from the merger of the Home Team Behavioural Sciences Centre, the Office of Chief Psychologist, and the Centre for Advanced Psychological Sciences. HTPD comprises two directorates:

- Psychology Services Directorate, specialising in psychological assessment services
- Psychology Research Directorate, focusing on psychological research

The areas for services and research include leadership and talent psychology, mental resilience, criminal psychology, and community trauma in a crisis.

ACKNOWLEDGEMENTS

The authors would like to thank Chief Psychologist of the Home Team Psychology Division, Dr Majeed Khader; Director Ms Diong Siew Maan; and fellow deep specialist colleagues for their continuous guidance, support, and encouragement.

REFERENCES

- Abelson, H. I. (1959). *Persuasion: How opinions and attitudes are changed*. Springer Pub. Co.
- Albarracín, D., & Karan, A. (2022). Resistance to persuasion. *Oxford Research Encyclopaedia of Psychology*. <https://doi.org/10.1093/acrefore/9780190236557.013.813>
- Cialdini, R. B. (2021). *Influence: The psychology of persuasion*. Harper Business,
- Cohen, L. E., & Felson, M. (1979). Social change and crime rate trends: A routine activity approach. *American Sociological Review*, 44, 588-608. <http://dx.doi.org/10.2307/2094589>
- de Gregorio, F., Jung, J. -H., & Sung, Y. (2017). Advertising avoidance: A consumer socialization perspective. *Online Journal of Communication and Media Technologies*, 7(3). <https://doi.org/10.29333/ojcm/2597>
- Fransen, M. L., Verlegh, P. W. J., Kirmani, A., & Smit, E. G. (2015). A typology of consumer strategies for resisting advertising, and a review of mechanisms for countering them. *International Journal of Advertising*, 34(1), 6-16. <https://doi.org/10.1080/02650487.2014.995284>

- Friestad, M., & Wright, P. (1994). The persuasion knowledge model: How people cope with persuasion attempts. *Journal of Consumer Research*, 21(1), 1. <https://doi.org/10.1086/209380>
- Hollis-Peel, M. E., Reynald, D. M., van Bavel, M., Elffers, H., & Welsh, B. C. (2011). Guardianship for crime prevention: A critical review of the literature. *Crime, Law and Social Change*, 56, 53-70. <https://doi.org/10.1007/s10611-011-9309-2>
- 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), 1-7-122. <https://doi.org/10.1080/08946566.2013.821809>
- Johnson, J. P. (2013). Targeted advertising and advertising avoidance. *The RAND Journal of Economics*, 44(1), 128-144. <https://doi.org/10.1111/1756-2171.12014>
- Leclerc, B., Smallbone, S., & Wortley, R. (2013). Prevention nearby: The influence of the presence of a potential guardian on the severity of child sexual abuse. *Sexual Abuse*, 27(2), 189-204. <http://doi.org/10.1177/1079063213504594>
- Lim, J. (2022, July 30). Seniors will help other seniors spot scams under new initiative. *The Straits Times*. <https://www.straitstimes.com/singapore/courts-crime/new-anti-scam-initiative-involves-seniors-teaching-peers-how-to-spot-warning-signs>
- Ministry of Home Affairs. (2022, July 30). *Launch of Project PRAISE (Police-RSVP Anti-Scam Engagement) 2022: Speech by Ms Sun Xueling, Minister of State, Ministry of Home Affairs and Ministry of Social and Family Development* [Press Release]. <https://www.mha.gov.sg/mediaroom/speeches/launch-of-project-praise-police-rsvp-anti-scam-engagement-2022/>
- Reynald, D. (2009). Guardianship in action: Developing a new tool for measurement. *Crime Prevention and Community Safety*, 11(1), 1-20. <https://doi.org/10.1057/cpcs.2008.19>
- Sampson, R., Eck, J.E., & Dunham, J. (2010). Super controllers and crime prevention: A routine activity explanation of crime prevention success and failure. *Security Journal*, 23(1), 37-51. <https://doi.org/10.1057/sj.2009.17>
- ScamAlert. (2020). Scammer, beware: Building societal resilience to scams. *Home Team Behavioural Sciences Centre*. <https://www.scamalert.sg/resources/e-book>
- Singapore Counselling Centre, S. C. C. (2002, February 28). *Scams: Types, impact & avoiding them*. Counselling Services by Singapore Counselling Centre. Retrieved April 25, 2022, from <https://scc.sg/e/scams-types-impact-how-to-avoid-them/>
- Singapore Police Force (2022). Mid-Year Crime Statistics 2022. *Statistics*. <https://www.police.gov.sg/media-room/statistics>
- Singapore Police Force (2021). Annual Crime Brief 2021. *Statistics*. <https://www.police.gov.sg/media-room/statistics>
- van Sintemaartensdijk, I., van Gelder, J., van Prooijen, J., Nee, C., Otte, M., & van Lange, P. (2021). Mere presence of informal guardians deters burglars: A virtual reality study. *Journal of Experimental Criminology*, 17, 657-676. <https://doi.org/10.1007/s11292-020-09430-1>
- Venter, E. (2019). Challenges for meaningful interpersonal communication in a digital era. *HTS Theological Studies*, 75(1), 1-6. <https://doi.org/10.4102/hts.v75il.5339>
- Walther, J. B. (1996). Computer-mediated communication: Impersonal, interpersonal, and hyperpersonal interaction. *Communication Research*, 23(1), 3-43. <https://doi.org/10.1177/009365096023001001>
- Zuwerink-Jacks, J., & Cameron, K. A. (2003). Strategies for resisting persuasion. *Basic and Applied Social Psychology*, 25(2), 145-161. https://doi.org/10.1207/s15324834basop2502_5

THRIVE – A PSYCHOLOGICAL SUPPORT FRAMEWORK FOR POLICE INVESTIGATORS

Neo Hui Fang Samantha, Alyah Dinah Zalzuli, Athena Rachel Willis,
Ho Hui Fen & Jansen Ang
Police Psychological Services Department, Singapore Police Force

ABSTRACT

Policing work is known to be challenging and stressful, particularly for officers dealing with investigation. Research has found that homicide detectives or investigators dealing with sex crimes tend to suffer from secondary traumatic stress, given the frequent exposure to traumatic materials in their line of work. At the same time, the investigation of such cases tends to attract both internal and external scrutiny which contribute to the cumulation of fatigue and psychological strain. Given the unique stressors faced by investigators, it is important to develop measures to support their mental health while increasing their resiliency to operate effectively. The Singapore Police Force has thus developed a psychological support framework known as THRIVE for its investigation community. The 3 x 3 THRIVE framework prescribes initiatives focusing on different levels – individual, supervisor, and organisation – and at different tiers – primary, secondary, and tertiary. The Police Psychological Services Department (PPSD) worked together with a team of paracounsellors to implement THRIVE interventions for the investigators. Preliminary evaluation of the THRIVE programmes suggest some efficacy in identifying at-risk groups or individuals, and mitigation of the risk of increased psychological harm to investigators. More efforts are required to sustain the initiatives and ensure adequate support is provided for investigators.

INTRODUCTION

Law enforcement work is widely acknowledged to be stressful and demanding (Queirós et al., 2020; Violanti et al., 2017). Police officers are subjected to a variety of operational and operational stressors such as fatigue from shift-work or over-time demands, prolonged exposure to traumatic incidents and public pressure (Ryu et al., 2020; Jackman et al., 2020), manpower shortages and being passed over for promotions (Jackman et al., 2020). While there are many different police vocations, the duties of police investigators are known to be more challenging and workload intensive (Tan et al., 2022). Due to the demands of investigation work, officers often make many personal sacrifices – loss of rest time, sleep and time with family members (Li et al., 2021) – to promptly resolve cases. Rising public expectations and the evolving nature of crime also

present investigators with additional challenges in responding with professionalism.

Investigators are also found to be at a higher risk of psychological injury, secondary traumatic stress, compassion fatigue, and burnout due to the nature of the job (Powell & Tomy, 2011; Violanti et al., 2016; Sokol, 2014). Police personnel who work closely with the investigators, such as computer forensics experts, digital forensic investigators, and analysts, have also been found to be as susceptible to secondary traumatic stress or vicarious traumatisation (Lavis, 2012; Sokol, 2014). The severity of these mental health concerns may be coupled with certain barriers in seeking help such as the fear of putting their career at risk or the perceived stigma of being weak (Papazoglou & Tuttle, 2018). It can be an added concern given that investigators have access to firearms.

There is a need to improve the mental health, well-being and support initiatives for investigators. In 2019, the Singapore Police Force (SPF) set up a workgroup comprising officers from the Criminal Investigation Department (CID) and Police Psychological Services Department (PPSD) to enhance support to investigators. The group developed a customised resilience framework called the THRIVE Framework.

THRIVE – A RESILIENCE FRAMEWORK FOR INVESTIGATORS

Referencing the SPF’s 4-R Resilience Framework (Poh & Ho, 2010) and the model behind preventive interventions (Greenfield & Shore, 1995), THRIVE is a 3 x 3 framework that focuses on three main level of interventions – primary, secondary and tertiary (see Figure 1). The tiered interventions differentiate the degree of impact of psychological mental health concerns on different groups of officers. Primary interventions target all investigators, with the aim of preventing occurrence of psychological concerns. Secondary interventions target the investigators who are at risk of developing psychological problems and aim to detect problems in the early stages. Tertiary interventions are scoped to investigators who have shown signs of psychological issues and aim to support the officers in the recovery process.

The aims of an investigation specific resilience framework are thus to

- (1) prevent the onset of psychological injury,
- (2) identify early signs of psychological injury and disrupt the progression, and
- (3) support officers who are affected in recovery.

To match the aims of the framework, the proposed interventions include

- (1) having proper support systems with ease of accessibility,
- (2) equipping supervisors with tools and skills to support officers, and
- (3) destigmatising psychological injuries.

To thrive is to flourish and perform well, even in challenging situations. The key meaning of the word ‘thrive’ entails the essence of resilience by withstanding the pressure that one experiences in life (Fletcher & Sarkar, 2013). Likewise, the initiative of THRIVE aims to inculcate the desired attributes that a resilient IO should have – Team Support, Healthy,

Figure 1. Attributes of THRIVE

Thriving officers who are/have:

T	EAM SUPPORT
H	EALTHY
R	ESILIENT
I	NVOLVED
V	ERSATILE
E	NERGIZED

Resilient, Involved, Versatile and Energised (see Figure 1).

These interventions are further tiered into three different levels – individual, supervisors and organisation (SPF). The initiatives are scoped based on their role, responsibility and commitment for psychological support. For instance, individuals are responsible for their own health and well-being whereas supervisors are responsible for leading and caring for them. The organisation bears responsibility for the well-being of employees through management support and policy development.

PRIMARY (PREVENTION)

Individual Level Initiatives

The initiatives focus on provision of general mental health information to

- (1) recognise signs and symptoms of stress and mental health concerns,
- (2) inculcate a range of positive coping methods,
- (3) develop basic peer support skills, and
- (4) know of available support avenues.

PPSD introduced a route of advancement of resilience training courses for investigators that are pegged at the various ongoing investigation courses. These courses are categorised into four levels, where Levels 1 and 2 focus on self-care and peer support (introduction) at individual level (see Figure 3).

Figure 2. Aims of THRIVE Framework

Aims of THRIVE	Primary	Secondary	Tertiary
Individual	<ul style="list-style-type: none"> Resilient individuals with a diverse range of coping mechanisms Adaptable and open to feedback and new experiences 	<ul style="list-style-type: none"> Insightful and responsible individuals who engage in self-care and know when to seek help 	<ul style="list-style-type: none"> Knowledge of support avenues
Supervisor	<ul style="list-style-type: none"> Trained supervisors to detect signs of mental health issues and management skills Supportive supervisors 	<ul style="list-style-type: none"> Capable in early problem detection Supportive of help-seeking behaviours Familiar with support-referral process 	<ul style="list-style-type: none"> Facilitation of flexible working arrangements for affected investigators
Organisation	<ul style="list-style-type: none"> Supportive organisational climate Adequate resources and training for work Knowledge of seeking help 	<ul style="list-style-type: none"> Cultivation of psychological safety in seeking support via unit management 	<ul style="list-style-type: none"> Provision of internal and external support avenues

Figure 3. Overview of the Resilience Training Courses

THRIVE Level Initiative	Level	Investigation Course Pegged Under	Course Modules
Individual	Level 1	Home Team Basic Investigation Course (HT BIC)	<ul style="list-style-type: none"> Common stressors as investigators Understanding personal coping strategies Tips on managing stress and practising self-care
Individual	Level 2	Home Team Intermediate Investigation Course (HT IIC)	<ul style="list-style-type: none"> Identifying signs of concern amongst peers Tips on providing support from peer-to-peer
Supervisor	Level 3	Home Team Advanced Investigation Course (HT AIC)	<ul style="list-style-type: none"> Identifying signs of concern within team Suicide intervention Emotional first aid
Supervisor	Level 4	Home Team Investigation Manager Course (HT IMC)	<ul style="list-style-type: none"> Common sources of stress and its impact on investigators Identifying signs of concerns Knowing how and when to intervene and support Suicide and crisis intervention

Figure 4. THRIVE Handbook

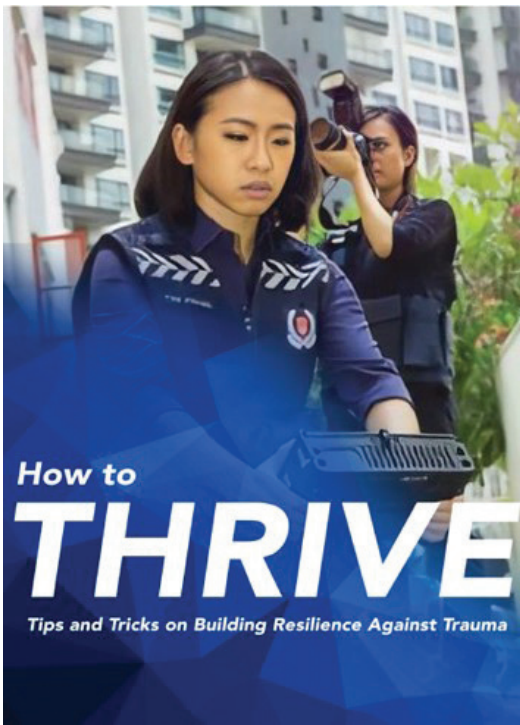


Table of contents

Introduction	05
How and why do people react after trauma?	07
Common traumatic situations	08
What is Post-Traumatic Stress Disorder?	13
Signs and symptoms of other related mental health concerns	19
Tips on managing Critical Incident Stresses	24
Improving resilience on a day-to-day basis	25
Preparing yourself before a case	35
Reducing traumatic effects after a case	44
Peers: How to Help?	40
Why am I important as a peer?	61
Tips on how to provide support as a peer	62
Supervisors: How to Help?	75
Why am I important as a supervisor?	76
What are the barriers to seeking help?	77
Encouraging a safe and open culture	78
Tips on supporting recovering officers	83
Where can I find further help?	85
Additional resources	89

In addition, a resource handbook on “Building Resilience against Trauma” was disseminated to the investigators to improve their resiliency against critical incident stresses. The handbook includes topics on identifying signs and symptoms of trauma, learning self-help skills on preventing and managing trauma, and acquiring skills to support someone affected by trauma (see Figure 4).

Supervisor Level Initiatives

Training modules comprising suicide awareness and critical incident management were introduced for investigators with supervisory roles. These courses are pegged under Levels 3 and 4 of the route of advancement, where the content of the courses focus on peer support (intermediate) and stress and crisis management respectively (see Figure 3). These modules provide supervisors with knowledge on spotting signs of distress among investigators, and how to engage them sensitively. Information on supporting the team during and post critical incidents (i.e., line of duty injuries or deaths) are discussed as well.

Organisation Level Initiatives

Specific stressors identified by investigators (e.g., manpower shortage, fatigue, etc.) led to the following organisational initiatives

- (1) mental health awareness week,
- (2) protected time-off, and
- (3) provision of recreation rooms.

A dedicated mental health awareness week for investigators (THRIVE Week) is held annually. It coincides with the World Mental Health Day (10 October). This week reminds leaders and investigators of the importance of mental health awareness, well-being, and self-care. To mark this week, the THRIVE workgroup designs and disseminates a series of broadcasts to enhance public education on destigmatising help-seeking behaviours, and to equip investigators and supervisors with knowledge of common psychological injuries for investigators, and skills on self-care and supervisory support (see Figure 5).

Figure 5. Broadcasts on Signs of Mental Health Concerns and Supervisory Support

World Mental Health Day

Theme: Mental Health in an Unequal World

In conjunction with the World Mental Health Awareness Day commemorated annually on 10 October, PPSD will be providing a series of information for awareness. In this first instalment, we will like to highlight some common mental health concerns. Do note the support avenues platforms for officers to seek help when the need arises.

1 Stress

- Stress occurs when we interpret a situation as more physically or mentally demanding than our resources to cope with it.
- It is a heightened state of tension and a natural bodily response to perceived threats.
- Short term impact of stress includes headaches, feeling overwhelmed, poor concentration, lack of motivation, etc.
- Chronic stress occurs when stress is not properly managed over prolonged time and symptoms include trouble sleeping, irritability, digestive problems, etc.




2 Anxiety

- Anxiety is characterised by feelings of uneasiness, worry or fear to an anticipated threat.
- Symptoms of anxiety include:
 - Very fast heartbeats
 - Muscle tension
 - Sense of impending danger
 - Feeling 'on edge' or nervous



3 Depression

- Depression is a mood disorder characterised by persistent feelings of sadness that can feel crippling and overwhelming to the point of interfering with everyday life.
- Feelings of sadness are a natural part of life. But if these feelings are persistent and interfere with daily functioning, one may require the facilitation of additional help.
- Symptoms include:
 - Low mood and hopelessness
 - Loss of interest in hobbies
 - Feeling empty or numb



HOW SUPERVISORS CAN HELP TO PREVENT THE ONSET OF MENTAL HEALTH CONCERNS

EASE OF SHARING

INCREASE THE EASE OF SHARING FOR OFFICERS SUCH AS SETTING A POSITIVE TONE, RESOLVING CONFLICTS EARLY AND QUICKLY, ETC

(REFER TO "TIPS TO ENCOURAGE OPEN COMMUNICATION WITHIN YOUR TEAM")

PROVIDING A POSITIVE & SUPPORTIVE ENVIRONMENT BY MONITORING & SUPPORT OFFICERS' WORKLOADS, ENCOURAGING OFFICERS TO TAKE BREAKS, ETC

(REFER TO "TIPS TO PROVIDE SUPPORT IN GENERAL")

HELPING RECOVERING OFFICERS TO TRANSITION BACK TO THEIR NORMAL WORK ROUTINES BY DISCUSSING WITH OFFICERS ON THE WORK THEY FEEL CAPABLE OF HANDLING DURING THEIR RECOVERY, ALLOWING TIME OFF, ETC

(REFER TO "TIPS ON SUPPORTING RECOVERING OFFICERS" & RESOURCES TO FIND FURTHER HELP")

BARRIERS TO SEEKING HELP

ADDRESS THE BARRIERS TO SEEKING HELP BY REDUCING THE STIGMA THAT SEEKING HELP IS A FORM A OF 'CAREER SUICIDE'

HAVE AN OPEN & HONEST DISCUSSION WITH OFFICERS ON ANY POSSIBLE IMPACTS ON THEIR CAREER IF THEY SEEK HELP. ADDRESS THEIR CONCERNS ON COUNSELLING, EMPHASIS ON CONFIDENTIALITY, ETC

(REFER TO "WAYS TO ADDRESS BARRIERS TO SEEKING HELP")

RESOURCES

Resources

- 24/7 PPSD CARE Helpline: 1800 265 1151
- PPSD CARE Email: PPSD.CARE@police.gov.sg (Email for managers only)
- WOO Counselling Helpline: 6865 9209 (For Unauthorised and Regular officers)

Brought to you by PPSD

Resources in the form of thumbs up magnets and encouragement postcards have been disseminated to investigators as part of the *SteadyLah!* Campaign. Feedback have been largely positive, with investigators noting that the resources serve as a

conversation starter amongst peers to check in with one another during stressful periods (see Figure 6).

To encourage a supportive climate within the divisions, the Deputy Head Investigation and Deputy

Figure 6. Reviews shared by IOs on the *SteadyLah!* Campaign

STEADYLAH! CAMPAIGN

THE STEADYLAH! CAMPAIGN WAS LAUNCHED ON 4 OCT 2021 AS PART OF AN ONGOING EFFORT TO SUPPORT ONE ANOTHER.

THUMBS-UP MAGNETS AND POSTCARDS WERE DISTRIBUTED TO OFFICERS.

THE THUMBS-UP MAGNET IS INTENDED TO BE USED FROM A FIRST PERSON'S PERSPECTIVE, REMINDING THE IO THAT WHILE MUCH IS EXPECTED OF THEM, **THEY ARE ONLY HUMAN** AND THEY ARE ENCOURAGED TO BE SEEN AND FELT.

THE POSTCARD REPRESENTS AN OUTSIDER'S PERSPECTIVE, TO PASS IT FORWARD WHEN THEY SEE A COLLEAGUE IN NEED OF **SOME ENCOURAGEMENT**. FROM THE READER'S PERSPECTIVE, THE IO WILL BE REMINDED THAT IT IS OK TO BE NOT OK.

CHECK OUT SOME OF THE FEEDBACK FROM THE OFFICERS!

I received a note from my branch mate. It is a quote, by William Jones to inspire. I wasn't expecting it but was pleasantly surprised to have received it.

Motivates me to remind my IOs to balance work and personal life.

I've written words of encouragement to lighten the mood and motivate fellow colleagues.

I placed the magnet at the front of the door so that the other IOs can be reminded that we have each other.

Messages of support have been given to fellow officers appearing to be down and jaded with work. It made them feel that they are not alone in this battle.

I was feeling down earlier in the day and displayed a "thumbs down". I received a note of encouragement and felt much better and happier!

Head of Branch of each division are nominated to be the **THRIVE champions** for their own unit-level THRIVE initiatives. Given their supervisory role, these officers serve a dual role of spreading the messages of care within their investigators, as well as in cultivating the culture of care in the longer term. A feedback survey conducted in September 2021, a year after the unit-level initiatives were implemented, showed the popularity of the various initiatives rolled out to the units. A video montage highlighting the top three units with higher levels of engagements was then shown during THRIVE Week to recognise the efforts of these units and to encourage other units to continue rolling out more of such initiatives (see Figure 7).

In response to suggestions from investigators, **protected time-off** was established in 2020 to address the fatigue arising from disrupted leave. A handbook on “Best Practices for Leave Taking” was subsequently created and disseminated to all investigators during the inaugural THRIVE Week in 2020. The handbook lists the roles and responsibilities of the investigator, Covering Officer(s) and Investigation Supervisor in minimising leave interruptions. Some of the responsibilities include the investigator preparing a proper handing over of outstanding cases before going on leave, the Covering Officer(s) having to assess the situation before interrupting the investigator on leave and lastly, the Investigation Supervisor checking first with the Covering Officer(s) instead of the investigator on leave.

Figure 7. Summary of Survey Results on Unit-Level THRIVE Initiatives



CID has also created a **new recreational safe space** for investigators known as R3 (Relax, Recharge and Reconnect). Made available in October 2022, the space provides the necessary reflection outlet for investigators, and support their social interactions with colleagues and the conduct of activities that hopefully bring about a positive change in their job satisfaction. The idea is to reduce the stressful emotions that may be associated with the workplace (Shujat, 2011).

SECONDARY (DETECTION)

Individual Level Initiatives

To encourage investigators who are at risk of psychological concerns to engage in self-care and seek help when they have issues, the THRIVE

workgroup designed and disseminated a series of broadcast messages to promote awareness on general mental health concerns for self and peer awareness. Additional information on basic support skills such as active listening skills, risk assessment of harm to self or others, assurance of available support avenues is provided in the infographics, for ease of reference when engaging a distressed colleague (see Figure 8). Materials and resources that are broadcasted during the THRIVE Week are also uploaded on a shared platform for easy reference by investigators.

Supervisor Level Initiatives

To help supervisors identify investigators who may have mental health concerns as early as possible and provide them the necessary interventions, SPF

Figure 8. Poster on Basic Support Skills for Investigation Officers

PEERS: HOW TO HELP?

Why am I important as a peer?

Social support from peers is one of the most effective protective factors against PTSD and compassion fatigue for police work. Take any communication of distress seriously. Remember that your role is **NOT TO TREAT OR DIAGNOSE** your peers, but **TO HELP THEM SEEK PROFESSIONAL HELP OR PROPER SUPPORT AS SOON AS POSSIBLE.**

How can I provide support as a peer?

1. Active listening skills
2. Risk assessment of harm to self or others
3. Imparting information and reassurance of help available
4. Providing social support

"Refer to the Trauma Handbook attached (Pg. 62-63)" to more detailed information.

Do you know how to adequately support your peers? Use the checklist below to find out:

1. Practising active listening skills (Page 62)
 - Do you show concern and listen to your peers without judging or giving advice?
 - Do you show that you're listening via non-verbal cues such as maintaining eye contact, nodding your head, etc.?
 - Do you paraphrase what you've heard to show understanding and clarify any misunderstandings?
 - Do you help to reflect your peer's feelings and allow them to express their emotions?
2. Conducting risk assessment (Page 64)
 - Do you know how to assess if someone is at risk of harm to themselves or others?
 - Do you know how to ensure the person's safety (Page 71) if you suspect that they are at risk?
3. Imparting information, reassurance and providing social support (Page 73)

Checklist: Tips for Peers

piloted the Police Resilience Assurance System (PRAS) in November 2021. The investigation units identified for the pilot run of PRAS included the Serious Sexual Crime Branch (SSCB) and the Crime Scene Squad (CSS) in the land divisions where investigators may be at higher risk of developing mental health concerns due to their job scope.

PRAS is backed by research showing that administering a screening process can help an organisation identify employees who may be having difficulty or are struggling at work (Aparacio et al., 2013; Ali, Ryan, & De Silva, 2016). Having a routine screening process may also help to destigmatise help seeking behaviour and normalise being psychologically injured (Police Executive Research Forum, 2019).

Organisation Level Initiatives

Besides PRAS, leaders are encouraged to have increased engagement with officers via informal dialogue sessions. Through these engagements, leaders can further emphasise the importance of mental health and cultivate psychological safety in seeking physical or mental support. Following dialogue sessions, leaders should update their officers on the follow-up measures so that the officers can feel that they are being heard and cared for. For example, senior SPF leaders i.e., Deputy Commissioner of Police (Investigation & Intelligence) and Director, Criminal Investigation Department sent out messages during THRIVE week to affirm the importance of mental health and to provide reassurance on help-seeking behaviours when required.

TERTIARY (SUPPORTING AFFECTED OFFICERS)

Individual Level Initiatives

SPF provides officers with multiple help seeking options, ranging from self-help, peer support and counselling services. Counselling services are available via helpline, in-person by unit paracounsellors or by PPSD, or external counselling service procured by Public Service

Figure 9. Available Resources for Help-Seeking

World Mental Health Day
Theme: Mental Health in an Unequal World

In conjunction with the World Mental Health Awareness Day commemorated annually on 10 October, PPSD will be providing a series of information for awareness. In this third instalment, we will like to highlight the possible avenues for seeking professional help to improve one's overall well-being and resilience during times of need.

SPF INTERNAL RESOURCES

- Unit Paracounsellors
 - Paracounsellors are trained in-house staff who are responsible for addressing mental health needs.
- Police Psychological Services Department (PPSD)
 - PPSD Helpline: 1800-354-111
 - Email: SPF_CARE_Office_Care@police.gov.sg

EXTERNAL RESOURCES

- Ministry of Government (MOG) Counselling Services by Public Service Division (PSD)
 - Call: 6552-2800 to enquire for an appointment
 - Visit: www.mog.gov.sg or www.psd.gov.sg for more information
 - Applicable for regular and casual employees
- Physicians can refer medical patients or non-registered hospital or GP patients to obtain assistance for specialist psychological psychiatric support

ONLINE RESOURCES

- Mindline SG
 - Free of charge
 - 24/7 available
 - Register as a user to access the service
- Mental Health Portal
 - Free of charge
 - 24/7 available
 - Register as a user to access the service

EXTERNAL HELPLINES

- National Crisis Helpline: 1800-222-6868
- Institute of Mental Health (IMH) Mental Wellness Helpline: 6355-2222
- Serious Mental Illness (SMI) Helpline: 1-767
- SCS CARE Line (Serious Mental Illness) Helpline: 6355-2222
- Singapore Association for Mental Health: 1900-265-2018
- Toughline Helpline for Government: 1800-377-2222
- TUOH Care Line for seniors caregivers: 6804-0200
- Safe Corner Counselling Centre: 1800-353-5800

Brought to you by PPSD
 Scan QR code for PPSD Telegram Channel

Division. All available support avenues are actively publicised, including the online repository of self-help materials (see Figure 9). Additionally, electronic posters advertising help services are disseminated via official email, and physical posters placed in high footfall areas (i.e., lift landings and bulletin boards). The resources available are also incorporated into all training modules. These are to encourage individual help seeking behaviours in officers.

Supervisor Level Initiatives

Once supervisors have identified, either through their daily observations or via PRAS, officers who may benefit from additional mental health support, they will first conduct an informal

check-in session with the officers. Thereafter, supervisors may evaluate the required support (i.e., facilitate re-assignment of workload or duties) during a period of recovery. Supervisors are also made aware of the referral processes to PPSD for internal counselling support or to Whole-of-Government counselling services. To enable these, supervisors are trained through the respective investigation milestone courses.

Organisation Level Initiatives

At the organisation level, PPSD has implemented various support avenues for officers. This includes an online repository of mental health materials which consists of self-help materials on anxiety, depression, and post-traumatic stress. Officers may access the intranet site to access these materials. If the officers are uncomfortable with seeking in-person support, they may reach out via the 24/7 helpline counselling or by email. A PPSD psychologist or trained senior paracounsellors can provide timely psychological support via these channels. Dedicated counselling support arrangements (involving forensic-trained PPSD officers whom CID investigators are familiar with) have also been implemented for higher risk units. Finally, investigators are provided the option to seek external support from the government's counselling service. At an organisational level, a system of mental health support has been established.

LESSONS LEARNT FROM THRIVE

Working with key stakeholders

The THRIVE Framework has been developed with the intent to provide better support to the investigation community given the stressors that they face. It is thus important to get the necessary buy-in from the key stakeholders within the investigation community so that the interventions can be sustained in the longer term. Working with relevant parties such as the Home Team School of Criminal Investigation to roll out the key THRIVE resilience modules, and with unit leaders on PRAS are also key to the success of the interventions.

Partnership with supervisors on providing care

Supervisors are often the first line of support for the officers on the ground. There are many benefits in partnering with supervisors to provide support to their officers. For instance, it can help to enhance their role as leaders in caring for their people, hence improving the overall ground support and morale of the officers. Such partnership with supervisors can also allow for early interventions, thereby lowering the occurrence of officers developing serious psychological concerns that require interventions from paracounsellors and psychologists. Overall, partnership with supervisors enhances the overall *in-situ* support for officers.

Leveraging on frameworks to guide resilience initiatives

By having a structured resilience framework for the investigation community, PPSD and CID unit management are better able to identify possible gaps and look at innovative ways to better improve systemic processes. It may be useful for other units or Home Team agencies to consider developing relevant frameworks for their officers and use the frameworks to explore possible ways to enhance their resilience initiatives on the ground. This provides a holistic support for investigators as opposed to ad-hoc stress management courses when officers are stressed.

CONCLUSION

Policing work is specialised and unique, hence a generic one-size-fits-all resilience approach would not work. A dedicated support framework, like THRIVE, is better able to meet the contextual psychological needs of investigators in the SPF. It can also help to guide officers in structuring their resilience and support interventions. As THRIVE continues to evolve and move into a steady state, it is important to ensure the sustainability of the interventions and to constantly evaluate the effectiveness of these interventions at different time points. With improvements and continual evaluation of the framework and its interventions, a psychologically safe and resilient work culture can be cultivated within the investigation community, leading to greater work performance and resiliency among the investigators.

ABOUT THE AUTHORS



Neo Hui Fang Samantha

holds a Master's degree in Health Psychology from King College London and a Bachelor's degree (with honours) of Social Sciences (Psychology) from National University of Singapore. She is currently the Lead Psychologist from the Resilience and Counselling Psychology Branch in the Police Psychological Services Department (PPSD), Singapore Police Force (SPF), as well as a forward deployed psychologist in the Training Command (TRACOM). Her main role includes providing counselling support to Police National Fulltime Servicemen (PNSFs) in TRACOM, conducting training for both PNSFs and supervisors, and managing the counselling and resilience efforts within PPSD and SPF. Samantha's research interests are in the areas of physical health, mental health, and wellness.



Alyah Dinah Zalzuli

holds an Honours Degree of Bachelor of Science (Psychology) from the University of Northampton. She is currently a Research Analyst (Resilience and Counselling Psychology Branch) in the Police Psychological Services Department (PPSD), Singapore Police Force (SPF). She is involved in projects and research studies on mental health of investigation officers and COVID-19 related psychological support. She is currently also working on creating a screening tool for investigation officers and helping with the management of the SPF Paracounselling Programme. Alyah's research interests are in mental health and well-being.



Athena Rachel Willis

holds a Degree (Honours) of Bachelor of Arts (Psychology) from University at Buffalo, New York. She is currently a Psychologist with the Resilience and Counselling Psychology Branch, Police Psychological Services Department (PPSD), Singapore Police Force (SPF). Her main roles include development of resilience programmes for specialist operators and investigation officers, management of counselling referrals, resilience efforts and the SPF Paracounselling Programme. Her research interests are in resilience and psychological well-being.



Ho Hui Fen

holds a Degree of Bachelor of Social Sciences in Psychology from the National University of Singapore and a Master of Science in Occupational Health Psychology from the University of Nottingham, United Kingdom. She is a registered graduate member of the British Psychological Society (BPS). She holds the Certificate of Competence in Occupational Testing (Level A and Level B) and is a qualified tester listed in the Register of Competence in Psychological Testing with the BPS. Hui Fen is currently the Assistant Director, Operations and Forensic Psychology Division in the Police Psychological Services Department (PPSD), Singapore Police Force (SPF). She oversees services relating to resilience psychology (e.g., counselling, paracounselling), operations psychology (e.g., morale sensing, employee engagement) and crime psychology (e.g., investigation support, crime research, victim care). Within the Ministry of Home Affairs, Hui Fen leads the Home Team Mental Health and Well-being Taskforce, looking into standards of practice for Home Team resilience and well-being psychological services. Hui Fen is also the Deputy Head CARE of the SPF in the National CARE Management System which manages psychological impact arising from national crises.



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 for the Police, Narcotics, Civil Defence, Prisons, Immigration & 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. In the Singapore Police Force, Jansen 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 organisational excellence in the police. He is also the Police's representative on the National CARE Management Committee that is the body responsible for managing the psychological impact arising from national crises and incidents. An Associate Professor (Adjunct) at the Nanyang Technological University in Singapore, he lectures on trauma psychology at the College of Humanities and Social Sciences. His 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.

ACKNOWLEDGEMENTS

The authors would like to express their thanks to the following officers from the Singapore Police Force who contributed to the development of the THRIVE Framework and the implementation of the initiatives:

- Tan Xuan Ting, Cheryl, Psychologist, Police Psychological Services Department
- Florence Chua, Former Deputy Commissioner of Police (Investigations and Intelligence)
- Lian Ghim Hua, Deputy Commissioner of Police (Operations)
- Zhang Weihan, Director, Police Intelligence Department
- Sam Lee Thai Ching, Deputy Head, Financial Investigation Branch, Criminal Investigation Department
- Crystal Ng Xiang Ning, Chief Investigation Officer (Development & Services), Woodlands Division
- Jason Gan Hong Teck, 2 Operations Officer (Crimes 3), Criminal Investigation Department
- Diana Tay Xue Ping, Staff Officer, Specialised Crime Policy Branch, Criminal Investigation Department
- Kevin Lee Ming Woei, Operations Officer, Operations Planning Branch, Investigation Development and Systems Division, Criminal Investigation Department
- Lee Pei Ling, Interpol (Former Head Technology Crime Branch, Criminal Investigation Department)

REFERENCES

Akhter, A., Mobarak Karim, M., & M. Anwarul Islam, K. (2021). The impact of emotional intelligence, employee empowerment and cultural intelligence on commercial bank employees' job satisfaction. *Banks and Bank Systems*, 16(4), 11–21. [https://doi.org/10.21511/bbs.16\(4\).2021.02](https://doi.org/10.21511/bbs.16(4).2021.02)

Ali G-C, Ryan G, De Silva MJ (2016) Validated Screening Tools for Common Mental Disorders in Low and Middle Income Countries: A Systematic Review. *PLoS ONE* 11(6): e0156939. doi:10.1371/journal.pone.0156939

Aparicio, E., Michalopoulos, L., & Unick, G. (2013). An Examination of the Psychometric Properties of the Vicarious Trauma Scale in a Sample of Licensed Social Workers. *Health & Social Work*, 38(4), 199-206. doi: 10.1093/hsw/hlt017

- Charman, S., & Bennett, S. (2021). Voluntary resignations from the police service: the impact of organisational and occupational stressors on organisational commitment. *Policing and Society*, 32(2), 159–178. <https://doi.org/10.1080/10439463.2021.1891234>
- Civilotti, C., Acquadro Maran, D., Garbarino, S., & Magnavita, N. (2022b). Hopelessness in Police Officers and Its Association with Depression and Burnout: A Pilot Study. *International Journal of Environmental Research and Public Health*, 19(9), 5169. <https://doi.org/10.3390/ijerph19095169>
- Fletcher, D., & Sarkar, M. (2013). Psychological Resilience: A Review and Critique of Definitions, Concepts, and Theory. *European Psychologist*, 18(1), 12–23. <https://doi.org/10.1027/1016-9040/a000124>
- Garbarino, S., Cuomo, G., Chiorri, C., & Magnavita, N. (2013). Association of work-related stress with mental health problems in a special police force unit. *BMJ Open*, 3(7), e002791. <https://doi.org/10.1136/bmjopen-2013-002791>
- Greenfield, S. F., & Shore, M. F. (1995). Prevention of Psychiatric Disorders. *Harvard Review of Psychiatry*, 3(3), 115–129. <https://doi.org/10.3109/10673229509017177>
- Jackman, P. C., Clay, G., Coussens, A. H., Bird, M. D., & Henderson, H. (2020). 'We are fighting a tide that keeps coming against us': a mixed method exploration of stressors in an English county police force. *Police Practice and Research*, 22(1), 370–388. <https://doi.org/10.1080/15614263.2020.1789463>
- Karlsson, I., & Christianson, S. (2003). The phenomenology of traumatic experiences in police work. *Policing-an International Journal of Police Strategies & Management*, 26, 419-438.
- Li, J. C. M., Cheung, C. K., Sun, I. Y., Cheung, Y. K., & Zhu, S. (2021). Work–Family Conflicts, Stress, and Turnover Intention Among Hong Kong Police Officers Amid the COVID-19 Pandemic. *Police Quarterly*, 25(3), 281–309. <https://doi.org/10.1177/109861112111034777>
- Magnavita, N., & Garbarino, S. (2013). Is Absence Related to Work Stress? A Repeated Cross-Sectional Study on a Special Police Force. *American Journal of Industrial Medicine*, 56(7), 765–775. <https://doi.org/10.1002/ajim.22155>
- Papazoglou, K., & Tuttle, B. (2018). *Fighting Police Trauma: Practical Approaches to Addressing Psychological Needs of Officers*. *SAGE Open*, 8(3), 215824401879479. doi: 10.1177/2158244018794794
- Poh, L. L., & H, H. F. (2010). The 4-R Approach To Resilience Building In The Singapore Police Force.
- Police Executive Research Forum. (2019). *An Occupational Risk: What Every Police Agency Should Do to Prevent Suicide Among Its Officers* (pp. 26, 34 - 36). Washington, DC.
- Powell, M., & Tomy, A. (2011). Life Satisfaction Amongst Police Officers Working in the Area of Child Abuse Investigation. *International Journal of Police Science & Management*, 13(2), 187-194. doi: 10.1350/ijps.2011.13.2.225
- Smid, G. E., der Meer, C. A. I., Olf, M., & Nijdam, M. J. (2018). Predictors of Outcome and Residual Symptoms Following Trauma-Focused Psychotherapy in Police Officers With Posttraumatic Stress Disorder. *Journal of Traumatic Stress*, 31(5), 764–774. <https://doi.org/10.1002/jts.22328>
- Sokol, Natalie Lynn, "Dirty Work: The Effects of Viewing Disturbing Media on Military Attorneys" (2014). *Theses, Dissertations, and Other Capstone Projects*. Paper 317. <https://cornerstone.lib.mnsu.edu/cgi/viewcontent.cgi?article=1316&context=etds>
- Tan, Y. S., Zalzuli, A. D., Ang, J., Ho, H. F., & Tan, C. (2022). Understanding the Workload of Police Investigators: a Human Factors Approach. *Journal of Police and Criminal Psychology*, 37(2), 447–456. <https://doi.org/10.1007/s11896-022-09506-w>
- Queirós, C., Passos, F., Bárto, A., Marques, A. J., da Silva, C. F., & Pereira, A. (2020). Burnout and Stress Measurement in Police Officers: Literature Review and a Study With the Operational Police Stress Questionnaire. *Frontiers in Psychology*, 11. <https://doi.org/10.3389/fpsyg.2020.00587>

Ryu, G. W., Yang, Y. S., & Choi, M. (2020). Mediating role of coping style on the relationship between job stress and subjective well-being among Korean police officers. *BMC Public Health*, 20(1). <https://doi.org/10.1186/s12889-020-08546-3>

Violanti, J., Fekedulegn, D., Hartley, T., Charles, L., Andrew, M., Ma, C., & Burchfiel, C. (2016). Highly Rated and most Frequent Stressors among Police Officers: Gender Differences. *American Journal of Criminal Justice*, 41(4), 645-662. doi: 10.1007/s12103-016-9342-x

Violanti J. M., Charles L. E., McCanlies E., Hartley T. A., Baughman P., Andrew M. E., Burchfiel C. M. (2017) Police stressors and health: a state-of-the-art review. *Policing: An Int J Police Strat Manag* 40(4):642–656

PSYCHOLOGICAL CRISIS SUPPORT THROUGH A PANDEMIC: THE ICA EXPERIENCE

Naomi Liew & Poh Li Li
Immigration & Checkpoints Authority

ABSTRACT

Crises are known to strain the functioning of a nation's public sector. It is thus important for public agencies to enact and implement psychological crisis support plans prior to crises to better manage the psychological aftermath of a crisis and eventually restore operational normalcy swiftly. The COVID-19 pandemic was a crisis that stretched both the physical and mental health of the employees of the Immigration & Checkpoints Authority (ICA) as they worked to maintain the organisation's operational effectiveness. This article documents the experience of applying ICA's Psychological Crisis Support Framework in response to the critical distress caused by COVID-19. The framework guides psychological interventions from two perspectives in the management of a crisis: (1) the groups of organisational stakeholders involved, and (2) the phases of a crisis. These perspectives intersect to form a 4x4 matrix that allows stakeholders to easily determine the interventions recommended for a specified period of the crisis. Limitations and future directions are also discussed from this application.

ICA – STAYING RESILIENT IN THE COVID-19 PANDEMIC

The first case of COVID-19 was reported in Singapore on 23 January 2020 (Tan et al., 2021). Given the high rates of infection and re-infection, and Singapore's high density where people live closely to one another, there was an imperative for the government to take a swift and strong strategic approach to managing the crisis. Within a few months of the disease hitting Singapore's shores, various measures such as border control, stay-home notice (quarantine), contact tracing, intensive temperature screening, and mask wearing were implemented (Abdullah & Kim, 2020; Tan et al., 2021). Nonetheless, Singapore registered an exponential growth of cases in the following months with the number of confirmed cases spiking in early March 2020, of which a fair proportion of cases were believed to be imported (Ministry of Health, 2020; Tan et al., 2021).

The Immigration & Checkpoints Authority (ICA) is responsible for securing Singapore's borders to prevent undesirable people and cargo from entering

the country (Immigration & Checkpoints Authority [ICA], 2020). Due to ICA's key function in securing our borders, most ICA officers are also deployed at the various air, sea, and land checkpoints to conduct security checks on travellers and cargo. With the spike of imported cases coming in from overseas, this meant that ICA officers were placed at the forefront to fight the pandemic by carrying out enhanced border control measures. ICA officers also took on additional roles inland, such as the enforcement of the Stay-Home Notice (ICA Annual, 2021).

The COVID-19 virus has rapidly evolved since it first emerged (Runwal, 2022). Due to the dynamic nature of COVID-19 pandemic, ICA and its officers have had to stay agile and resilient to deal with the evolving disease, operating environment, and border control policies. As an organisation, ICA has responded by building more resilient systems, processes, and people. This includes accelerating its transformation efforts to enable a safer, more secure, and seamless border clearance experience such as allowing self-screening of passports by travellers, enabling travellers to use iris and facial biometrics for

screening, and integrating the digital authentication of vaccination certificates in the SG Arrival Card e-Service etc. (ICA Annual, 2021). Regardless of system advancements, ensuring that its people stay mentally resilient amidst the challenges of COVID-19 remain key for the organisation.

Impact of COVID-19 on ICA Officers

A pandemic, like a critical incident or crisis, can significantly impact an organisation's operations and the mental health of its employees (Jacobs et al., 2019). A critical incident or crisis is a low probability but high impact event that is usually outside the range of normal human experiences (Crandall et al., 2013; Mitchell, 2004). Experiencing crises like COVID-19 can result in critical incident stress, which is "a state of cognitive, physical, emotional, and behavioural arousal that accompanies the stress reaction" (Mitchell, 2004, p. 3). ICA officers, being deployed in the frontline during the prolonged pandemic, have reported similar stressors as other frontline workers, such as fear of safety for themselves and their loved ones, and chronic stress resulting from a changing operating environment and intensified workload (Sritharan et al., 2020). These stressors, if left unattended, can have a significant impact on those who experience it, resulting in more long-term psychological disorders such as Post Traumatic Stress Disorder (PTSD), depression, anxiety, and

substance-abuse (Mitchell, 2004). As ICA recognises the importance of maintaining and enhancing the mental resilience of its officers, it has been providing psychological crisis support to officers affected by the pandemic via a holistic system. This article details the development of the Psychological Crisis Support Framework (PsychCSF) for the ICA and how it has been applied to effectively support ICA officers affected by the COVID-19 crisis.

THE PSYCHOLOGICAL CRISIS SUPPORT FRAMEWORK

Formulated by ICA's in-house psychological services unit, the Psychological Crisis Support Framework (PsychCSF) is structured around two perspectives: (1) groups of stakeholders (i.e., individual employees, leaders, psychologically-trained responders, psychological services unit), and (2) phases of a crisis (pre-crisis, acute, response, recovery).

How a critical incident impacts an organisation may evolve over the period of the crisis. Therefore, accounting for both perspectives helps ICA adapt the psychological support needed by the different groups at each phase of the crisis. This in turn increases efficacy of the support. The 4x4 matrix (see Table 1) shows the types of psychological crisis support that fall in the intersections of the two perspectives.

Table 1. Psychological Crisis Support for the Groups of Organisational Stakeholders according to the Phases of Crises (4X4 Matrix)

(1) Groups of Organisational Stakeholders	(2) Phases of Crises			
	Pre-crisis	Acute	Response	Recovery
Individual Employees	Psychological preparation to anticipate critical distress	Reminders to refer to educational materials for coping with distress	Provided educational materials facilitating awareness for symptoms of post-traumatic distress, and how to manage them. Receiving psychological support from others who have undergone crisis	Provided educational materials to shift perspective of critical incident distress into post-traumatic growth

(1) Groups of Organisational Stakeholders	(2) Phases of Crises			
	Pre-crisis	Acute	Response	Recovery
Leaders	Psychological preparation to anticipate critical distress and guidance on managing employees in uncertain work climate	Provided bite-sized information on psychological risk symptoms and avenues to seek support for employees Reminded to refer to materials on crisis communication with employees	Encouraged to provide recognition and appreciation to employees Received feedback from team through recurring morale sensing exercises and trigger appropriate support needed	Looking out for vulnerable employees and monitoring psychological well-being of employees previously affected negatively Facilitating clarity in the uncertain work climate
Psychologically-trained Responders	Being trained for and Refreshed on Basic Psychological Support Skills and Morale-sensing skills Put on standby for potential activations to support colleagues	Deployed to monitor for affected colleagues and direct them to avenues of help	Tasked to provide emotional and practical support to reduce the probability of worsening psychological well-being.	Deployed to continue monitoring for affected teammates and direct them to avenues of help
Psychological Services Unit	Developing and disseminating material tailored to groups of organisational stakeholders to educate on mental health management Planning for recurring organisational feedback exercises	Regular check-ins with leaders and psychologically-trained responders Providing focused psychological support to employees who displayed risk	Extending group debriefing sessions to promote healthy psychological processing of a crisis Extending individual counselling support to employees who were survivors of crisis	Regular check-ins with psychologically-trained responders Standing down and debriefing psychologically-trained responders from their psychological support duties Providing resources for easier access to help Establishing ways of communication with wider community

APPLYING PsychCSF DURING THE COVID-19 PANDEMIC

Taking reference from PsychCSF, the following paragraphs detail the psychological support efforts provided to and by the stakeholders in ICA since

the beginning of the COVID-19 pandemic in 2020 to 2022 when the COVID-19 safe management measures started easing (Ministry of Health, 2022). With each phase of the crisis, the support efforts were adapted to provide for different stakeholder needs. Additionally, the nature of the crisis-at-hand

(a pandemic) caused many physical limitations to providing psychological support. Traditional psychological crisis support efforts had to be modified to cater to the social distancing regulations of the pandemic.

Pre-crisis support efforts for stakeholders

The pre-crisis phase refers to the period before the onset of critical distress. In the COVID-19 pandemic this was when reports of local COVID-19 cases first started to surface. At pre-crisis, the following support efforts were provided to and undertaken by the various groups of stakeholders.

Individual Employees

For the individual employee, building up personal resilience is a key objective of the pre-crisis support. Bonanno (2004) explains that an individual's resilience has positive influence on their personal psychological recovery after a crisis. Building up resilience and a sense of preparedness has been shown to mitigate the negative impact (e.g., trauma symptoms and negative interpretations) of critical incidents (Adams & Boscarino, 2006; Boscarino, 2015; Boscarino et al., 2011; Bonanno, 2004). As such, preparing ICA's employees psychologically for the imminent crisis involved IPS distributing educational materials that would help build employees' personal resilience against the fear and anxiety surrounding COVID-19. When news outlets reported the first few local COVID-19 cases, educational materials covering topics like detecting 'fake news' about the virus, methods to manage anxiety, and daily healthy coping strategies were disseminated digitally, through work email, agency-related messaging platform channels, and push-down screensavers for work on computers (see Figure 1).

Leaders of the Agency

Aside from receiving support, leaders in the agency could also be providing psychological support because they are symbols of order and authority in a critical incident (Seeger et al., 2003; Steigenberger, 2016). Supportive and effective leadership in a workplace increases role clarity, self-efficacy, and job engagement and thus mitigates the effects of potential stressors (Britt et al. 2004, Birkeland

Figure 1. Educational materials distributed through the Telegram messaging platform

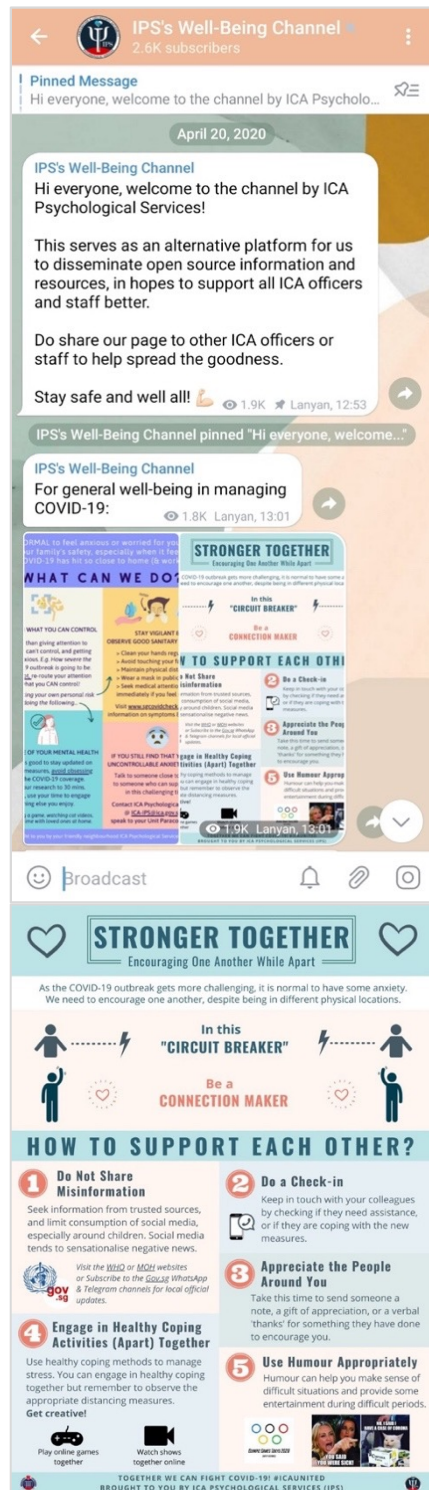


Figure 2. Educational materials on leadership in crisis for leaders of the agency

HEART TO HEART TALK SERIES 1/3

CRISIS LEADERSHIP & TEAM MANAGEMENT

Leadership. Not a duty, but an inevitable RESPONSIBILITY.

In this COVID-19 pandemic, our leaders have heavy responsibilities to ensure smooth running of ICA's core operations, and lead their team and organisation safely out of the storm. We have curated key areas of leadership which would be useful to help our leaders weather through the storm.

Be Adaptable.

Crisis takes place unexpectedly and can deteriorate fast unless a decision is made to manage it. Time can be critical, therefore **ADAPT BOLDLY**. One can never plan for all crises, but failing to plan for one can be detrimental. Hence, **ADOPT FLEXIBILITY** by having a wide range of responses at your disposal and be creative because sometimes unconventional and even unorthodox methods may prove to be effective in a unique situation.

BROADEN PERSPECTIVES, not just your own, but also your team members in light of the situation ahead. Look beyond the problem that is in front of you as there could be other challenges or opportunities that could present itself from the situation. List it all down and do not brush off issues that may seem insignificant. Be calm and assess how best to approach the situation.

Make Effective Decisions.

Analysis paralysis can easily result when there is cognitive overload, incomplete information, and when interests and priorities clash. There is a need to focus on the few things that matter most. **DEFINE YOUR PRIORITIES** clearly. Doing so in a logical manner can also aid you when you need to communicate priorities to others.

Do not be afraid to be **ASSERTIVE** and put on hold operations that are not critical at this moment (e.g. focus on the urgent and important things). **EMPOWER** your people to become decision makers as having centralised decision making can hinder work processes. State expectations clearly and set clear guidelines to help your people know which decisions they have authority over, and when they require higher authorisation. Focus on **EMBRACING ACTIONS**, and try not to punish mistakes.

"If you can't fly, then walk. If you can't walk, then crawl. But by all means, keep moving." - Martin Luther King Jr.

"I never worry about action. Only inaction." - Winston Churchill

"Where we are not with opinion and doubt, and those who believe that what we can't, we will respond with that timorous censure that burns up the spirit of a people. 'Yes, we can'." - Barack Obama

Employees do not come first. Employees come first. If you take care of your employees, they will take care of the clients." - Richard Branson

Brought to you by ICA Psychological Services (IPS)

HEART TO HEART TALK SERIES 1/3

Communicate With A Mind & Heart.

People will turn to leaders for instructions and they will want to know what is next. Leaders have to be mindful in how they communicate, so that disseminated messages do not elicit further panic. Start by **ADDRESSING THE EMOTIONS**. People who are upset are less able to grasp nuances, so be empathetic and acknowledge the fear and anxiety that people are experiencing. This will help them feel understood and ready to absorb the information you are providing.

Keep messages **CLEAR & UNAMBIGUOUS**, as people do not trust what they do not understand. Try to repeat, and reinforce your messages - in the era of "fake news", your consistency will be a beacon in times of distress.

Provide **PRAGMATIC ACTIONS** to help team members focus during times of uncertainty. Articulate the mission, and let people know what they can help. Some examples can be to encourage officers to seek and contribute to each others' well-being, and support facts instead of spreading misinformation.

Manage Your Teams.

While you take charge of the evolving situation, don't forget about managing your team's emotions and enhancing the team unity. In this pandemic, try to prioritise **EMPATHY, SAFETY & HEALTH**. Find ways to aid team members who need support in the short and long term, such as those who require extra time-off to source for day-care for children, or needing to care for elderly family members. Continue to provide guidance for members to navigate challenges.

Highlight **TEAM EFFORT & POSITIVITY**, as people hope best when they focus less on themselves and think about the welfare of others. Share significant contributions of officers and staff in ICA to illustrate that we are working as a team, and not in silo.

Use **LANGUAGE TO UNITE**, to reinforce the message that you are on the journey together with your team (e.g. "we", "us"). Avoid chastising members with "mistakes" to deter undesired behaviours as this can greatly affect morale. Don't forget to check in with individual team members to have a sensing on their states of mind, along with the week's highlights and low points.

Brought to you by ICA Psychological Services (IPS)

HEART TO HEART TALK SERIES 3/3

MANAGING STRESS IN A CHANGING OPERATIONAL ENVIRONMENT

IPS's Outreach for COVID-19

Since the onset of the COVID-19 outbreak, ICA has experienced many **CHANGES** in our operational work. Be it having to work longer hours, having to deal with new and evolving SOPs, or even having to take on new types of work and duties.

Changes are stressful journeys to go through for you and the people around you. **Nonetheless, know that some stress is normal in the process of change!**

The Journey through Change

Change evokes many different reactions. This model shows us people's usual reactions to change vs. their **morale & confidence** through time. Expectedly, morale & confidence dips when change is first introduced. However, it can rise again with effective leadership & personal management strategies.

Perhaps you or your colleagues have experienced one of these reactions:

<p style="text-align: center;">DENIAL (OR SHOCK)</p> <p>In this stage, you would feel lost & overwhelmed. You don't know what to do with all the new work.</p>	<p style="text-align: center;">ANGER (OR SADNESS)</p> <p>You feel strong negative emotions towards the change. You might be angry or demoralised by all of it. Usually people contemplate giving up & changing jobs.</p>	<p style="text-align: center;">EXPLORATION</p> <p>You carry out the change because you realised that you have to, but you also start thinking about a better way to tackle this change.</p>	<p style="text-align: center;">ACCEPTANCE</p> <p>In this stage, you have understood the need for change. You are dealing with it head-on & involved in improving the change behaviour.</p>
---	---	--	---

Brought to you by ICA Psychological Services (IPS)

HEART TO HEART TALK SERIES 3/3

What can you do as a leader to support people through the different reactions?

<p>Denial (or Shock)</p> <p>Give Informational and Practical Help:</p> <ul style="list-style-type: none"> ■ Share the trigger for the change (e.g. "There has been an increase in imported COVID-19 cases. Which is why we need to put in new SOPs") ■ Share the purpose for the change (e.g. "It will be extra work. But, it will also be preventing an influx of new cases into Singapore that can compromise the safety of Singaporeans, and maybe our families") ■ Share the future picture with this change in place (e.g. "This might only be the start of the changes, which might last at least 6 months. But know it all serves to keep the safety of our residents and our families.") ■ Provide additional guidance even when they make mistakes 	<p>Anger (or Sadness)</p> <p>Give the Team and Individuals Emotional Support:</p> <ul style="list-style-type: none"> ■ Avail yourself as a listening ear ■ Make time if someone approaches you to talk. If you are unable to make time then, Remember to get back to them. ■ Be deliberate and genuine in asking about how someone is coping with the change. ■ Adopt an open mind and allow your colleague to speak, don't interrupt with the solutions just yet ■ Provide peer support at work (e.g. a mentor, a paracounselor) to monitor and guide the individual out of the anger or sadness
<p>Exploration</p> <p>Give Clear Direction:</p> <ul style="list-style-type: none"> ■ Be consistent with instructions ■ (Or) Communicate the reasons for the continuously evolving instructions ■ Model desired attitudes towards change ■ Model the appropriate operational behaviors that has changed ■ Remind the team of the mission's goal 	<p>Acceptance</p> <p>Give Encouragements:</p> <ul style="list-style-type: none"> ■ Create a feedback mechanism for future changes (e.g. encourage honest responses in Morale Sensing. Avoid shutting down or punishing "negative" feedback) ■ Continue to thank people for keeping in pace with the changes even after it has been enacted.

Overall, keep the conversation about changes neutral and open throughout all the reactions. Invite feedback about change, genuinely consider it in your context, and address it no matter whether the individual is reacting in the anger or in acceptance. Doing so may help build trust in your leadership, and improve the outcome of change.

Brought to you by ICA Psychological Services (IPS)

et al., 2016; Iversen et al., 2008, Richins et al., 2020). Therefore, leaders may buffer the impact of post-crisis distress by influencing the reduction of fear and anxiety, minimising situational uncertainty with information, exemplifying recovery, and facilitating smoother transitions back to normalcy by fostering trust, shared values, and attitudes within the agency (Dunning, 1999; Iverson et al., 2008; Kowalski, 2019; Paton et al., 2000;

Vaughan & Tinker, 2009). In preparation for the crisis, leaders in ICA were provided with educational materials on detecting psychological distress in their employees, communicating change while allaying fears, and employing crisis leadership strategies (see Figure 2). These materials were disseminated through email campaigns and webinars with leaders of all levels starting from teams to those in the senior management.

Figure 3. Existing resources converted to be available virtually and adapted to social distancing measures

Counselling Resources in ICA

As humans, there are times when we may struggle with emotional difficulties, life challenges, or even mental health concerns. That is where counselling can be beneficial for you or your colleagues around you, by learning how to cope with the emotional distress and learn skills to address your problems. We have our share of ups and downs, and it is totally fine to seek help!

DID YOU KNOW?

- ICA has an **in-house counselling service**, managed by ICA Psychological Services (IPS). For Self or Supervisor-Referred face-to-face counselling (option of Online Counselling for follow ups), email us at ICA-IPS@ica.gov.sg.
- ICA also provides **External Counselling Service with Parkway**, for those who would prefer seeking face-to-face support elsewhere. Call **1800 738 9595** to book an appointment.
- PSD rolled out a **Counselling Hotline** for all public service officers since 1st March 2021. For over-the-phone or face-to-face counselling, call **6865 9209**.

• For more information, contact IPS at ICA-IPS@ica.gov.sg.
 • For more resources, head to the IPS google site at <https://go.gov.sg/ipsresources>, or scan here

DARE TO CARE
 You Can Make A Difference

During this period of difficult change, you & your colleagues may experience loneliness or sense a lack of communication & understanding within the team. **Care & compassion** can also be a priority alongside our work commitments. However, a culture of care can only be established when each of us makes the effort to support one another in times of need & uncertainty. Thus, we hope the tips below can encourage you to take small steps to establish a culture of care.

1 MAINTAIN MEANINGFUL SOCIAL INTERACTIONS

Telecommuting may seem to push us further apart into our individual comfort zones and prolonged periods can result in loneliness. When such feelings appear, take comfort in the use of technology & remind yourself to look forward to MORE connections when the situation improves.

- ESTABLISH REGULAR CONTACT WITH COLLEAGUES**
 through Skype/Zoom to see and hear each other. You could even arrange one evening per week to do a catch-up session with them.
- SUPPORT THOSE WITHOUT INTERNET ACCESS**
 Share used internet-surfing devices (e.g. handphones, laptops, tablets etc.) and guide them along or fall back onto traditional methods of having group calls on mobiles instead.
- DISTRIBUTE RESPONSIBILITIES OF LOOKING OUT FOR ONE ANOTHER**
 Use a buddy system to add a layer of mutual support. Ask buddies to do regular check-ins to engage & support each other.

2 ESTABLISH PSYCHOLOGICAL SAFETY

"Psychological safety is a belief that one will not be punished or humiliated for speaking up with ideas, questions, concerns or mistakes". Thus, if communication appears to consistently fail within the team, perhaps consider taking small steps in changing the culture instead!

- DEMONSTRATE INTEREST IN UNDERSTANDING YOUR TEAM**
 Simple actions like nodding & smiling on Skype/Zoom can show that you care about what others are saying.
- INITIATE DISCUSSIONS & CONSIDER EVERYONE'S FEEDBACK IN DECISION-MAKING**
 This keeps the team involved & engaged, while reminding them that there is still trust & transparency despite the unpredictable times. E.g. you could acknowledge feedback & seek to hear from everyone instead of only those who are vocal, etc.
- LEAVE KIND REMINDERS**
 Send encouraging messages to your team to make them feel appreciated!
- GROW TOGETHER**
 Celebrate milestones & share rewards as a team.

3 THINK IN EACH OTHERS' SHOES

When your colleague or leader has a different perspective from you, it can be difficult to understand where they're coming from and continue to have a civil discussion with them. So what can you do?

- **Accept** that people can have different perspectives and beliefs from you.
- Practice **active listening**. Don't listen with intents to judge, discredit or disprove the other person. Instead, consider their thoughts, feelings & intentions as they share their point of view.
- Momentarily **set aside your thoughts** about the matter and focus on tuning in the information shared.
- Ask questions with an **open mind** to get some clarity.

With the new information and understanding, it could reduce conflict, and it'll be easier to converse with the same person again in future!

BROUGHT TO YOU BY ICA PSYCHOLOGICAL SERVICES (IPS)

Psychologically-trained Responders

Another group of stakeholders are ICA employees who have been trained to (i) gather feedback on the organisation's psychological health and morale (the Unit Morale Sensing Team) and, (ii) deliver basic psychological crisis support such as peer social support, psychological first aid, and advocating support resources (the paracounsellors) available to their peers. During critical incidents, they are deployed to provide psychological support to their colleagues as support roles with an element of peer relationships have proven to be useful in mitigating post-crisis distress and lower PTSD risk (Coulombe et al., 2020; Fuglsang et al., 2004; Ozer, Best, Lipsey & Weiss, 2003;). In the COVID-19 pandemic, these responders were refreshed

on their basic psychological support skills with adjustments for social distancing measures (see Figure 3) and prepared for activation of support for their colleagues. Whilst on standby to support, they helped to ensure the educational materials for employees reached their colleagues and began exemplifying healthy coping strategies to those working with them.

Psychological Services Unit Within Agency

Finally, the ICA Psychological Services Unit (IPS) oversaw the deployment of the various psychological crisis support efforts. The IPS tailored interventions to the agency's operational environment for a more coordinated crisis response. As noted by Poh and Diong (2021) on in-situ psychologists providing psychological support to the Singapore Civil Defence Force, a psychological services unit embedded within an agency is able to proactively provide psychological support before critical distress worsens. In anticipation of the long-drawn impact of COVID-19, the IPS planned for recurring organisation-wide morale sensing exercises. Through morale sensing exercises, employees' sentiments are collated and shared with leaders to inform efforts for targeted support to the employees.

Acute support efforts for stakeholders

The acute phase refers to the onset of a crisis, which correlated to the months where COVID-19 cases were spiking within ICA, and employees faced heightened threats of contracting COVID-19 from increased contact with members of public. Adding to the anxiety was a frustration amongst employees concerning the rapid changes in key operational procedures.

Individual Employees

In the acute phase of a crisis, manpower is typically diverted to the essential operational duties of the organisation. Thus, there should be refrain from introducing new strategies for psychological support. During this phase in ICA, employees were

reminded of the educational materials disseminated earlier to them (see Figure 4). Repackaged into bite-sized messages, these materials were disseminated digitally with particular emphasis on messaging platforms (i.e., *Telegram* channels and *WhatsApp* groups) so they could be accessed by the officers at any time.

Leaders in the agency

Leaders were urged to create a supportive environment for recovery by communicating clearly with their teams. Particularly amidst the fast-changing operational procedures, they were reminded to provide their teams with frequent updates on the crisis and how it might affect the operational details. To help them, leaders were also provided with bite-sized materials on creating a shared purpose for the team, spotting possible psychological risk symptoms in their members, and the appropriate avenues of help available.

Psychologically-trained Responders

As responders were needed in their primary operational duties, they were not deployed to provide psychological support. Rather they were tasked to monitor for signs of distress amongst their colleagues (i.e., those on quarantine order and those on duty at work) and refer them to the appropriate help avenues.

Psychological Services Unit Within Agency

In this phase, psychological crisis support efforts were largely provided by the psychologists from

Figure 4. Push-down desktop screensaver on mindfulness



IPS. Beyond coordinating the development and dissemination of educational material for the various stakeholders, the IPS provided individual counselling to employees who were experiencing elevated distress in this period. In keeping with the goal of creating a supportive environment for recovery, the IPS was available for consultation with leaders on ways to do so when they had team members experiencing critical distress. Finally, the IPS also conducted regular check-ins with the psychologically-trained responders and leaders to monitor their ability to cope.

Response support efforts for stakeholders

The response phase follows and refers to the period where employees begin coping better with the effects of a crisis. During the pandemic, this was when leaders and psychologically-trained responders were accustomed to the process of monitoring and supporting employees. Although the number of COVID-19 positive cases might be still of concern, employees were also growing more familiar with the rapid operational changes.

Individual Employees

For most, psychological distress is a normal transient response to crisis. Negative reactions to crisis usually resolve within four to twelve weeks post-crisis and is mitigated with some psychological interventions (Cahill & Potoski, 2005). Thus, to improve the prognosis of post-crisis distress, support initiatives by the IPS were aimed at boosting an individual's healthy coping strategies. Some of these included increasing opportunities for colleagues to develop a supportive culture for one another (e.g., the IPS set up a virtual gratitude board for employees to provide and receive encouraging messages), disseminating educational materials to create awareness of symptoms of distress and how to manage them, virtual reminders of the available avenues of support, and encouragement to actively improve their working environment by participating in the morale-sensing exercises.

Leaders in the agency

As discussed in the pre-crisis phase, leaders of an organisation are in a position to create a workplace environment that bolsters recovery from post-crisis distress. Hence, ICA leaders were urged to

offer recognition and appreciation for the work accomplished by their teams throughout the pressure of a crisis (e.g., via email or messenger application mentions, modest tokens of appreciation delivered to employees, and virtual team bonding activities). Additionally, addressing workplace difficulties is an equally significant part of providing psychological support. As such, leaders sought feedback from their teams (through the recurring morale sensing exercises) and met their needs with the appropriate support (e.g., recognising that inaccessibility to workplace systems was impeding tasks and setting up remote access to key intranet systems).

Psychologically-trained Responders

Psychologically-trained responders play a significant role in forming a supportive workplace environment for recovery from critical stress. In ICA, responders were readily deployed to provide basic psychological support to colleagues impacted by the crisis (i.e., employees who were quarantined away from family, employees who contracted COVID-19, team members who had to manage the loss of manpower). They were assigned to monitor and provide emotional support to their colleagues through their quarantine period. When necessary, responders arranged for practical help (e.g., delivering food, attending to an urgent matter at the colleague's home). After the quarantine, responders also briefly monitored their colleagues' adjustment back to work. Aside from delivering basic psychological support, responders facilitated communication between employees and their leaders by executing morale-sensing exercises (formal feedback) and gathering informal feedback through conversations with colleagues around them.

Psychological Services Unit Within Agency

The IPS coordinated and ensured the deployment of support to the quarantined employees as they received their COVID-19 quarantine orders (i.e., isolating away from the public and immediate household members). They assigned responders to each quarantined employee, and delivered a daily timed message to encourage and nudge them to practise healthy coping strategies during quarantine. Separately, as the responders supported their colleagues, the IPS in turn supported the group of responders by monitoring

their well-being and triaging for more complex cases. For employees with complex circumstances or greater distress responses, the IPS extended targeted support initiatives such as group critical stress debriefing and individual counselling.

Recovery support efforts for stakeholders

The recovery phase refers to the period where the organisation returns to the operational state before the crisis. For the pandemic experience in ICA, this occurred towards the beginning of the year 2022 as the nationwide social distancing measures began to relax (Ministry of Health, 2022).

Individual employees

Even when operational procedures begin reverting to the pre-crisis state, any change may still surface stress reactions as employees re-adapt. In preparation for the prolonged stressors, an individual's perspectives on coping should shift from an emphasis on functioning adequately to viewing distress as growth. This mindset is also known as post-traumatic growth, which is understood as the experience of positive change resulting from a struggle with challenging crises in life (Tedeschi & Calhoun, 2004). In studies across various crisis settings, factors that improve the emergence of post-traumatic growth are the adoption of spirituality, optimism for the future, positive reappraisal coping, and the presence of supportive others (Cadell et al., 2003; Prati & Pietrantoni, 2008; Schultz et al., 2010). Therefore, in this phase, ICA employees were provided educational materials that focused on facilitating positive reinterpretation and giving meaning to the crisis, as well as ways to engage and support one another at the workplace.

Leaders in the agency

Leaders smoothen the transition back into pre-crisis operations by maintaining a supportive workplace environment. ICA leaders were urged to continue monitoring their team's well-being, especially of those who were previously affected by the crisis. As leaders may facilitate post-traumatic growth in their employees, they were encouraged to offer updates on changes in operations and to chart the team's work goals moving forward.

Psychologically-trained Responders

In the recovery phase, responders pared back their support and only looked out for vulnerable colleagues, referring them for more targeted psychological support if needed. These structures for detection and support are kept as there is a possibility of the late onset of critical stress symptoms.

Psychological Services Unit Within Agency

The IPS continued extending the targeted psychological support of critical incident debriefing and individual counselling. They also disseminated reminders of the avenues for psychological support available to the organisation. As studies have documented possible secondary distress from supporting in a crisis, the well-being of responders is also important (Agentero & Setti, 2010; Palm et al., 2004; Trippany et al., 2004; Waegemakers & Lane, 2019). With that in mind, IPS held regular check-ins and debriefing sessions with the psychologically-trained responders as they completed their support work.

DISCUSSION

The PsychCSF guided implementation of psychological crisis support efforts during ICA's experience of the COVID-19 pandemic. This experience surfaced several learning points in the successful application of the framework.

Firstly, despite the framework including several support groups, critical incidents are dynamic and psychological support efforts would especially benefit from an overseeing body to coordinate and adapt the support efforts to the crisis-at-hand. In the framework, the role was proposed to be taken on by the psychological services unit embedded within the organisation; for ICA this was the ICA Psychological Services (IPS). One of the major adjustments that had to be made during the COVID-19 crisis was the mode of delivery for psychological crisis support.

The unexpected impediment to physical contact during the pandemic resulted in the IPS having to digitise internal processes and innovate ways of communicating and engaging the organisation with psychological support. Existing information on resources was ported to mobile messaging

platforms (e.g., *Telegram*) for employees to access on-the-go, new mediums for information dissemination (e.g., podcasts, videos, webinars) were employed, and there was a shift to using virtual tools for targeted psychological support (e.g., counselling on the *Zoom* app), ensuring that employees could receive the appropriate crisis support despite the circumstances. However, since these developments were novel and unfamiliar to the organisation and its employees, there was an inherent period of transition and adaptation before employees embraced the new systems and processes. Despite this, there were others who still preferred the traditional face-to-face support, and adjustments were made to provide support to them with risk mitigation measures in place, especially for cases deemed to be high risk. Nonetheless, as the organisation returns to pre-crisis operations, these new modes of support are kept in anticipation of future crises.

In the same vein, developing and maintaining various crisis support capabilities in the periods outside of the crisis phases is essential for timely and effective crisis response. Although not mentioned as part of the framework, the level of personal resilience previously developed significantly moderates the experience of present adversity and its effects on mental well-being (Seery et al., 2010; Seery et al., 2013) – suggesting that individual resilience should be built over time and way before the onset of crises. The IPS had made such efforts to promote resilience in the organisation before the COVID-19 pandemic began, thus easing the enhancement of resilience during the COVID-19 outbreak. Similarly, the psychologically-trained responders and leaders who act as a system of social support (associated with better mental health during outbreaks) (Pan et al., 2005; Tam et al., 2004; Xiao et al., 2020) will take time to develop social connections needed in crisis support. More practically, employees who are responders require time to be trained and proficient in the basic psychological crisis support skills and morale-sensing procedures. As such, the psychological support efforts sustained beyond a crisis is advantageous to the timeliness of psychological responses in future crises.

LIMITATIONS AND FUTURE DIRECTIONS

Supporting ICA through the COVID-19 pandemic has also raised possible challenges to note in the

application of PsychCSF for future crises. Firstly, even though critical incidents will likely cycle through all four crisis phases, each phase may not be so clearly distinguishable from the next. This could then affect the timeliness of certain support efforts being triggered. For future crises, employees' overall morale could serve not just as a feedback process between leaders and their teams, but also as an indicator of the crisis phase (e.g., morale sensing results show an increasing trend in employees' coping – indicating a shift into the response phase). Therefore, establishing the organisation's surveying capabilities early would allow stakeholders to monitor employee morale and overcome this limitation.

Another challenge may be that the preparations needed for implementing the PsychCSF is laborious. Organisations that take on this framework may be found in a critical incident before stakeholders can be prepared (e.g., employees not trained with basic psychological support skills). Nonetheless, **organisations should, at the earliest possible time, acknowledge and promote the concept of psychological well-being as a function of organisational performance.**

Finally, future studies should consider the level of impact the PsychCSF support efforts have on post-crisis distress and uncover the support initiatives that are most effective in mitigating distress. Creating a feedback loop for each crisis encountered would allow for continuous improvement to the framework.

CONCLUSION

Psychological crisis support targeting the psychological well-being of employees should be of paramount concern for organisations with operational capabilities that may encounter crises. ICA recognises the potential threats of critical stress on the psychological well-being of their employees and in turn its operational capabilities. The PsychCSF is a way for the organisation to mitigate the negative impact of critical incidents more effectively. Beyond crises, the Framework would also inculcate psychologically informed practices and a culture of support throughout the whole organisation and reinforce the importance of mental well-being in operations.

ABOUT THE AUTHORS



Naomi Liew

is a psychologist with the ICA Psychological Services (IPS). She obtained her Bachelor of Social Science (Hons) in Psychology at Nanyang Technological University. Her current work in IPS involves leadership training, development, and evaluation with the aim of growing ICA leaders to their potential as they continue their leadership journey. Previously, Naomi oversaw the operations and development of ICA's Paracounselling cadre and drove related mental resilience work for ICA. When she is not being a psychologist, she can be found hunched over her crafting table working on a mish-mash of projects to display in her home.



Poh Li Li

is the Deputy Director and Senior Principal Psychologist with the ICA Psychological Services (IPS). She attained her Master of Social Sciences (Psychology) from the National University of Singapore. Having a strong interest in clinical and helping work, she is presently pursuing a part-time doctorate in clinical psychology with the James Cook University. She also has a passion for leadership work, believing that all of us have the potential to become better leaders in our fields. In her free time, she enjoys arts and craft, from drawing on her iPad, to jewellery making and crocheting.

REFERENCES

- Abdullah, W. J., & Kim, S. (2020). Singapore's response to the COVID-19 outbreak: A critical assessment. *American Review of Public Administration*, 50(6-7) 770–776. <https://doi.org/10.1177/020275074020942454>
- Adams, R. E., & Boscarino, J. A. (2006). Predictors of PTSD and Delayed PTSD After Disaster. *The Journal of Nervous and Mental Disease*, 194(7), 485–493. doi:10.1097/01.nmd.0000228503.95503.e9
- Argentero, P., & Setti, I. (2010). Engagement and Vicarious Traumatization in rescue workers. *International Archives of Occupational and Environmental Health*, 84(1), 67–75. doi:10.1007/s00420-010-0601-8
- Boscarino, J. A., Adams, R. E., & Figley, C. R. (2011). Mental Health Service Use After the World Trade Center Disaster. *The Journal of Nervous and Mental Disease*, 199(2), 91–99. doi:10.1097/nmd.0b013e3182043b39
- Boscarino J. A. (2015). Community Disasters, Psychological Trauma, and Crisis Intervention. *International journal of emergency mental health*, 17(1), 369–371.
- Bonanno, G. A. (2004). Loss, Trauma, and Human Resilience: Have We Underestimated the Human Capacity to Thrive After Extremely Aversive Events? *American Psychologist*, 59(1), 20–28. doi:10.1037/0003-066x.59.1.20
- Britt, T. W., Davison, J., Bliese, P. D., & Castro, C. A. (2004). How leaders can influence the impact that stressors have on soldiers. *Military medicine*, 169(7), 541-545.
- Cadell, S., Regehr, C., & Hemsworth, D. (2003). Factors contributing to posttraumatic growth: a proposed structural equation model. *The American journal of orthopsychiatry*, 73(3), 279–287. <https://doi.org/10.1037/0002-9432.73.3.279>
- Crandall, W. R., Parnell, J. A., and Spillan, J. E. (2013). A Framework for Crisis Management. In *Crisis Management: Leading in the new strategy landscape* (pp. 1 - 19). SAGE.
- Cahill, S. P., & Pontoski, K. (2005). Post-traumatic stress disorder and acute stress disorder I: their nature and assessment considerations. *Psychiatry (Edgmont)*, 2(4), 14–25.

Coulombe, S., Pacheco, T., Cox, E., Khalil, C., Doucerain, M. M., Auger, E., & Meunier, S. (2020). Risk and Resilience Factors During the COVID-19 Pandemic: A Snapshot of the Experiences of Canadian Workers Early on in the Crisis. *Frontiers in psychology*, 11, 580702. <https://doi.org/10.3389/fpsyg.2020.580702>

Dunning, C. (1999). "Post-intervention strategies to reduce police trauma: a paradigm shift", in Violanti, J.M. and Paton, D. (Eds), *Police Trauma: Psychological Aftermath of Civilian Combat*, Charles C. Thomas, Springfield, IL.

Fuglsang, A. K., Moergeli, H., & Schnyder, U. (2004). Does acute stress disorder predict post-traumatic stress disorder in traffic accident victims? Analysis of a self-report inventory. *Nordic Journal of Psychiatry*, 58(3), 223–229. doi:10.1080/08039480410006278

ICA Annual (2021). *Securing our borders, safeguarding our home*. <https://www.ica.gov.sg/news-and-publications/ica-annuals>

Immigration and Checkpoints Authority [ICA] (2020). *Vision, mission & values*. <https://www.ica.gov.sg/about-us/vision-mission-values>

Iversen, A. C., Fear, N. T., Ehlers, A., Hacker Hughes, J., Hull, L., Earnshaw, M., Hotopf, M. (2008). Risk factors for post-traumatic stress disorder among UK Armed Forces personnel. *Psychological Medicine*, 38(4). doi:10.1017/s0033291708002778

Jacobs, J., Oosterbeek, M., Tummers, L. G., Noordegraaf, M., Yzermans, C. J., & Dückers, M. L.A. (2019). The organization of post-disaster psychosocial support in the Netherlands: a meta-synthesis. *European Journal of Psychotraumatology*, 10(1), 1544024. doi:10.1080/20008198.2018.1544024

Kowalski, C. (2019). Leadership of first-responders following trauma. *Journal of business continuity & emergency planning*, 13(1), 81–90.

Mitchell, J. T. (2004). Crisis intervention and critical incident stress management: A defense of the field. *Research Gate*. https://www.researchgate.net/publication/265190414_Crisis_Intervention_and_Critical_Incident_Stress_Management_A_defense_of_the_field

Ministry of Health (2020). *Additional precautionary measures to prevent further importation and spread of COVID-19 cases 13th March 2020*. <https://www.moh.gov.sg/news-highlights/details/additional-precautionary-measures-to-prevent-further-importation-and-spread-of-covid-19-cases>

Ministry of Health (2022). *Resuming our transition to resilience*. 11 March 2022. <https://www.moh.gov.sg/news-highlights/details/resuming-our-transition-to-resilience>

Moore, S. (2021). *History of COVID-19*. <https://www.google.com/amp/s/www.news-medical.net/amp/health/History-of-COVID-19.aspx>

Ozer, E. J., Best, S. R., Lipsey, T. L., & Weiss, D. S. (2003). Predictors of posttraumatic stress disorder and symptoms in adults: A meta-analysis. *Psychological Bulletin*, 129(1), 52–73. doi:10.1037/0033-2909.129.1.52

Palm, K. M., Polusny, M. A., & Follette, V. M. (2004). Vicarious Traumatization: Potential Hazards and Interventions for Disaster and Trauma Workers. *Prehospital and Disaster Medicine*, 19(01), 73–78. doi:10.1017/s1049023x00001503

Pan, P. J., Chang, S. H., and Yu, Y. Y. (2005). A support group for home-quarantined college students exposed to SARS: learning from practice. *Journal for Specialist in Group Work*, 30, 363–374. doi: 10.1080/01933920500186951

Paton, D., Smith, L., & Violanti, J. (2000). Disaster response: risk, vulnerability and resilience. *Disaster Prevention and Management: An International Journal*, 9(3), 173–180. doi:10.1108/09653560010335068

Poh, H. W., and Diong, S. M. (2021). The role of psychologists in supporting Singapore's urban search and rescue contingent in overseas missions. *Crisis, Stress, and Human Resilience: An International Journal*. 2(4), 168–72.

Prati, G., and Pietrantoni, L. (2009). Optimism, Social Support, and Coping Strategies As Factors Contributing to Posttraumatic Growth: A Meta-Analysis, *Journal of Loss and Trauma*, 14(5), 364-388, DOI: 10.1080/15325020902724271

Richins, M. T., Gauntlett, L., Tehrani, N., Hesketh, I., Weston, D., Carter, H., & Amlôt, R. (2020). Early post-trauma interventions in organizations: A scoping review. *Frontiers in Psychology*, 11. <https://doi.org/10.3389/fpsyg.2020.01176>

Runwal, P. (2022). *Two years into the pandemic, COVID-19 still surprises experts*. <https://www.google.com/amp/s/api.nationalgeographic.com/distribution/public/amp/science/article/two-years-into-the-pandemic-covid-19-still-surprises-experts>

Schultz, J. M., Tallman, B. A., & Altmaier, E. M. (2010). Pathways to posttraumatic growth: The contributions of forgiveness and importance of religion and spirituality. *Psychology of Religion and Spirituality*, 2(2), 104–114. <https://doi.org/10.1037/a0018454>

Seeger, M.W., Ulmer, R.R., Novak, J.M. and Sellnow, T. (2005), "Post-crisis discourse and organizational change, failure and renewal", *Journal of Organizational Change Management*, 18(1), 78-95. <https://doi.org/10.1108/09534810510579869>

Seery, M. D., Holman, E. A., & Silver, R. C. (2010). Whatever does not kill us: Cumulative lifetime adversity, vulnerability, and resilience. *Journal of Personality and Social Psychology*, 99(6), 1025–1041. <https://doi.org/10.1037/a0021344>

Seery, M. D., Leo, R. J., Lupien, S. P., Kondrak, C. L., & Almonte, J. L. (2013). An upside to adversity?: moderate cumulative lifetime adversity is associated with resilient responses in the face of controlled stressors. *Psychological science*, 24(7), 1181–1189. <https://doi.org/10.1177/0956797612469210>

Sritharan, J., Jegathesan, T., Vimalaswaran, D., & Sritharan, A. (2020). Mental Health Concerns of Frontline Workers During the COVID-19 Pandemic: A Scoping Review. *Global Journal of Health Science*, 12(11), 89. <https://doi.org/10.5539/gjhs.v12n11p89>

Steigenberger, N. (2016). Organizing for the Big One: A Review of Case Studies and a Research Agenda for Multi-Agency Disaster Response. *Journal of contingencies and crisis management*, 24(2), 60-72. <https://doi.org/10.1111/1468-5973.12106>

Tam, C. W., Pang, E. P., Lam, L. C., and Chiu, H. F. (2004). Severe acute respiratory syndrome (SARS) in Hong Kong in 2003: stress and psychological impact among frontline healthcare workers. *Psychological Medicine* 34, 1197–1204. doi: 10.1017/S0033291704002247

Tan, J. B., Cook, M. J., Logan, P., Rozanova, L., & Wilder-Smith, A. (2021). A Singapore's pandemic preparedness: An overview of the first wave of COVID-19. *International Journal of Environmental Research and Public Health*, 18, 252. <https://doi.org/10.3390/ijerph18010252>

Tedeschi, R. G., & Calhoun, L. G. (2004). Target Article: "Posttraumatic Growth: Conceptual Foundations and Empirical Evidence". *Psychological Inquiry*, 15(1), 1–18. https://doi.org/10.1207/s15327965pli1501_01

Trippany, R. L., Kress, V. E. W., & Wilcoxon, S. A. (2004). Preventing Vicarious Trauma: What Counselors Should Know When Working With Trauma Survivors. *Journal of Counseling & Development*, 82(1), 31–37. doi:10.1002/j.1556-6678.2004.tb00283.x

Vaughan, E., & Tinker, T. (2009). Effective Health Risk Communication About Pandemic Influenza for Vulnerable Populations. *American Journal of Public Health*, 99(S2), S324–S332. doi:10.2105/ajph.2009.162537

Waegemakers Schiff, J., & Lane, A. M. (2019). PTSD Symptoms, Vicarious Traumatization, and Burnout in Front Line Workers in the Homeless Sector. *Community mental health journal*, 55(3), 454–462. <https://doi.org/10.1007/s10597-018-00364-7>

Xiao, H., Zhang, Y., Kong, D., Li, S., and Yang, N. (2020). The effects of social support on sleep quality of medical staff treating patients with coronavirus disease 2019 (COVID-19) in January and February 2020 in China. *Medical Science Monitor*, 26, e923549–e923541. doi: 10.12659/MSM.923549

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

Hasan 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 and uses 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 outfit of ExCEL and how they support operational, research, and conditioning/corrective training functions.

DOUBLING DOWN ON SAFETY AND PERFORMANCE

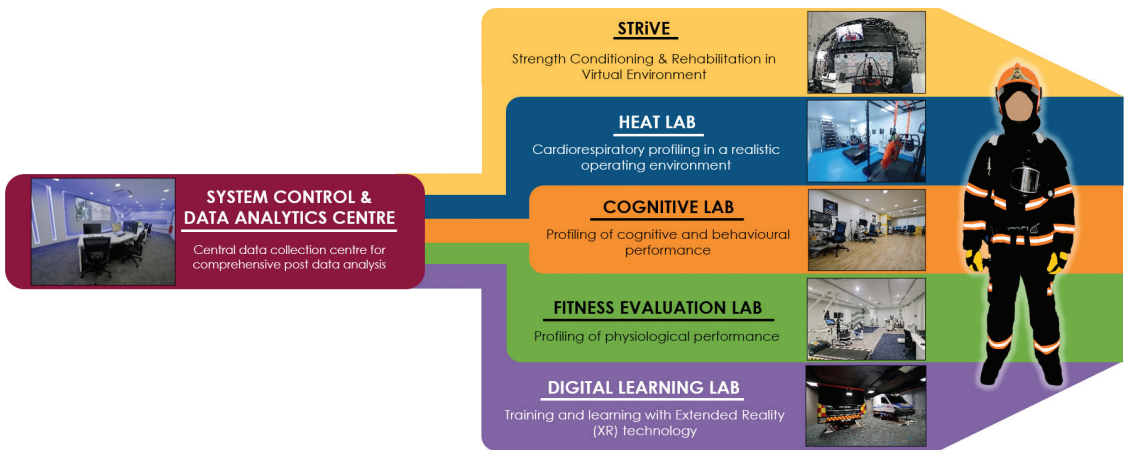
Emergency responders are often required to attend to cases with agility and strength to mitigate an incident effectively. As the demand for emergency response continues to rise due to Singapore's ageing population, the challenge for the Singapore Civil Defence Force (SCDF) is to boost its ability to 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 testing – 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 analysis, 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:

- Situational awareness training for firefighting and rescue operations;
- Assessment and characterisation of muscle activation patterns in different operational

- techniques, such as the proper methods to lift heavy equipment and proper running form;
- Conditioning for uneven terrains, e.g., stimulating rough sea states during motion acclimatisation training for responders in marine units;
- Evaluation and optimisation of load carriage and exoskeleton systems;
- Profiling and analysis of responders' gait patterns to predict fatigue rate or injury risks; and
- 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

HEAT ACCLIMATISATION & THERMOREGULATION (HEAT) LAB

- Simulate desired climatic conditions
- Temperature ranges from -10°C to 80°C
- Enable a wide range of realistic training scenarios and research studies
 - Thermal-physiological studies
 - Acclimatisation
 - Breathing Apparatus Proficiency Test (BAPT)



the Breathing Apparatus Proficiency Test (BAPT) regime. Set in an environmental chamber that simulates the desired climatic conditions (such as temperature, relative humidity, and wind speed), the HEAT lab enables a wide range of training scenarios in a realistic yet controlled environment. With a temperature range from -10°C to 80°C and a humidity level between 20% and 95%, responders are able to experience extreme climatic conditions for acclimatisation prior to deployments for overseas missions that could lead to potential heat or cold stress. An adaptive thermal physiology programme also allows researchers to study how environmental factors affect physical performance, and serves as a testbed for research pertaining to the effectiveness of personal protective gear.

Review of the BAPT Regime

Tapping into the new capabilities afforded by the HEAT lab, the BAPT regime was reviewed to improve the assessment of the cardiorespiratory and thermal fitness of firefighters. Frontline responders in the fire and rescue vocation are expected to complete and pass the BAPT regime annually to certify that they are fit for operational duties. In this regard, the new BAPT regime is designed to simulate the physical and physiological demands of actual firefighting; specifically, three new test stations have been introduced to replace the 'Impact Machine', 'Bicycle Ergometer', and 'Running Belt Ergometer'.

BREATHING APPARATUS PROFICIENCY TEST

The BAPT is an annual requirement of SCDP's frontline responders to maintain their cardio-respiratory and thermal fitness as firefighters. The new BAPT regime comprises 3 new test batteries in replacement of the Impact Machine, Bicycle Ergometer, and Running Belt Ergometer.

BEFORE REVIEW



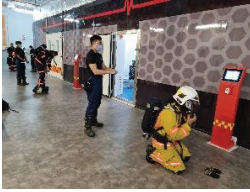

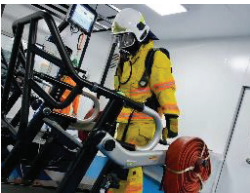



AFTER REVIEW



- Ops Task Relevance
- Performance Optimisation
- Enhanced Safety



Table 1. Six Stations of the BAPT Regime

Test Station		Test Requirement
BA Donning		Don full Personal Protective Equipment (PPE) and Self-Contained Breathing Apparatus (SCBA) within 1 min and 15 secs
Endless Ladder		Ascend 24m up the ladder
Hose Carry (new)		Walk a distance of 50m while carrying 2 x 64mm hoses
Stairs Climb (new)		Climb 24m or an equivalent of 8 storeys
Casualty Carry (new)		Perform a backward drag of a casualty weighing approximately 50kg over a distance of 30m
BA Maze		Navigate through the maze – 120m search and rescue obstacle course with configurable modules

Together with the BA Maze, the full BAPT regime consists of six stations (see Table 1). The BA Donning and BA Maze are the first and final stations respectively, while the four static stations can be completed in any sequence. Responders are to complete the BAPT regime with 240 bars of oxygen in the Breathing Apparatus. To ensure

the new BAPT regime is driven by evidence-based findings to achieve operational task relevance, performance optimisation and enhanced safety, a trial was conducted in collaboration with HTX and local academic institutions. An overview of the methodology can be seen in Table 2.

Table 2. Trial Protocol & Methodology for new BAPT Regime

Objectives		Methodology
Phase 1A	<ul style="list-style-type: none"> Determine maximal Volume of Oxygen (VO₂) and Heart Rate (HR) of trial participants Formulated via predictive approach* (non-intrusive) 	<ul style="list-style-type: none"> Estimate max VO₂ and HR using 2.4km timing and participants' age respectively
Phase 1B	<ul style="list-style-type: none"> Evaluate whether the new test stations can elicit physiological response similar to ops condition across all age groups (i.e., 60-80% VO₂max and >80% HRmax)** 	<ul style="list-style-type: none"> Attempt individual static stations at minimum baseline standards to measure VO₂ and HR response across different age groups and gender Allow HR to return to resting HR before next station
Phase 2	<ul style="list-style-type: none"> Assess completion rate of the new BAPT regime within the duration of one BA cylinder Establish a scoring system for the new BAPT regime 	<ul style="list-style-type: none"> Participants undergo full BAPT assessment Measure rate of completion and completion timing for the new BAPT regime

*Formula used (Trinh, 2019): $VO_{2max} = 76.775 - (2.543 * Run\ Time\ [mins])$

** Studies have reported that firefighters commonly work between 60-80% of their Maximum Volume of Oxygen (VO₂max) and more than 80% of their Maximum Heart Rate (HRmax) when performing operational tasks.

Findings of BAPT Review

All static stations on average were observed to have elicited 60 to 80% VO₂max and >80% HRmax. Trial participants from all age groups were within the target parameters, and were able to complete the BA Maze within 12 minutes. The majority also consumed less than 240 bars of oxygen at Phase 2, with a completion rate of 76.7%.

With the above findings, the new BAPT regime was rolled out in May 2022 with the adoption of the trial standards as a pass/fail requirement for responders to attain familiarisation with the new test stations. The formalisation of the regime as a graded qualification will be deliberated on as the limitation in the sample size made it difficult to establish a comprehensive scoring framework.

COGNITIVE LAB

The Cognitive Lab comprises a series of experimentation and behavioural systems to study and enhance the cognitive performance and situational awareness of responders. Test panels and audio-visual cameras are strategically placed to monitor and capture behavioural patterns of responders in a given scenario.

The lab utilises a variety of technology in combination with classical experimental methods, and is primarily equipped with advanced optical brain monitoring and imaging systems such as the Functional Near-Infrared Spectroscopy (fNIRS) and Eye Tracking System (ETS). The fNIRS helps in the profiling of mental workload in relation to specific tasks and training activity, while the ETS evaluates visual scan patterns and

NEW BAPT REGIME



WHAT TO EXPECT?

01



SELF-REGISTRATION

02

1 MIN 15 SEC



BA DONNING

03

CHAMBER CONDITION
28°C AT 60% HUMIDITY



STATIC STATION

24M



STAIR CLIMB

24M



ENDLESS LADDER

50M



HOSE CARRY

30M



CASUALTY CARRY

3 MIN TO COMPLETE EACH
STATIC STATIONS

2 MIN MANDATORY REST TIME
BETWEEN STATIC STATIONS

04

12 MIN



BA MAZE



CONSUME
<240BARS

REQUIREMENT

PASS

OR

FAIL

NO
GRADING

NO AGE
CATEGORY

NOT
GENDER
BIASED



helps responders to focus and achieve a thorough appreciation of the situation. The latter can also be used to profile the effectiveness of virtual reality and simulation training.

The Cognitive Lab includes a Psychomotor Vigilance Test (PVT) tool to chart the attention and

fatigue changes throughout the different task types or training regimes. By identifying the timepoints at which attention typically wanes, work-rest cycles can be refined for an optimal and effective deployment of responders.

Fitness Evaluation Lab

The Fitness Evaluation Lab employs scientific procedures to measure key components of physical fitness, and is an avenue for responders to optimise their performance as it analyses a range of components from strength to agility. The facility is furnished with:

- a. Isokinetic and isometric multi-joint and grip dynamometers to assess muscular strength;
- b. An integrated metabolic measurement system to assess cardiorespiratory endurance;
- c. A bioelectrical impedance analyser for body composition analysis;

- d. A vertical jump testing system for lower-body power measurements; and
- e. A dual beam timing system to assess speed and reactive agility.



- b. Mixed Reality (MR) Road Traffic Accident rescue training module which enables responders to understand vehicle anatomy and learn or revise the various rescue techniques involved in the extrication of casualties in a virtual environment;
- c. XR pump operations training module – delivered via a head-mounted display device and can be extended to the frontline units – which allows responders to have repeated training of the workflow of different pumps in SCDF;
- d. VR firefighting training module which teaches responders the different types of fire phenomena and the corresponding tactical response required; and
- e. MR Emergency Medical Services (EMS) training module which enhances training

Such physiological fitness testing enables SCDF to identify a responder's predisposition to musculoskeletal injuries and customise individual-specific training needs. Pre and post-training data are also compared to evaluate the effectiveness of training regimes and modifications. In the long run, building a database of responders' physiological fitness data helps to set practical and realistic benchmarks for specialist vocations.

DIGITAL LEARNING LAB

The Digital Learning Lab (DLL) allows responders to learn through Extended Reality (XR) technology in a safe and controlled environment without constraints imposed by the physical environment. The lab comprises a driving simulator that provide responders the opportunity to practise emergency response driving of either a fire engine or an ambulance. The use of data analytics provides insights on a responders' performance to facilitate targeted or corrective training.

The DLL also includes the following capabilities:

- a. Virtual Reality (VR) fire investigation training module which replicates post-fire environments and provides forensic tools for a fully immersive training experience in virtual burnt rooms;

DRIVING SIMULATOR

CAPABILITIES

This system comprises a configurable Virtual Instrument Panel to mimic the different types of vehicle models, as well as motion platforms to simulate realistic driving conditions (such as road unevenness and collision impact) in a safe and controlled environment.





Test Route Familiarisation | Reinforcement Training | Scenario Driving Training | After Action Review

SOFTWARE SYSTEM KEY FEATURES

Detailed 3D City Model - Edited for Customised Training for more than 3 km



Geo-specific Terrain Database:

- High-fidelity graphics with multiple levels-of-detail (LOD) to enhance the visual immersive experience

Includes a host of road driving scenarios and incidents to hone the driving skills and risk awareness of trainees



Flexible Scenario Editor Tool:

- Includes a host of road driving scenarios and incidents to hone the driving skills and risk awareness of trainees

Provide insights on trainees' performance and driving behaviours to facilitate targeted or corrective training



Wide-ranging & Interactive Data Analytic Tool:

- Provide insights on trainees' performance and driving behaviours to facilitate targeted or corrective training
- Identify trainees' 'unsafe driving habits' for early intervention

TERRAIN DATABASE



Custom Operations Command



Raffles International School



Jurong ICB



Jurong Air Station



Singapore ICB

DATA ANALYTICS
Data Mining & Functions






realism and allows SCDF paramedics and Emergency Medical Technicians (EMTs) to accelerate training of on-scene assessment and pre-hospital treatment protocols.

These simulators in the DLL serve to elevate SCDF's training productivity and efficiency as the XR training arrangements are flexible and can be catered to the needs of the responder. Above all, it saves time and resources involved in the set-up of the physical training environment.

System Control & Data Analytics Centre

The System Control & Data Analytics Centre is the nucleus of ExCEL as it centrally controls all the systems and collates data from the various facilities for a holistic analysis of responder performance. The Test Results and Assessment Management System (TRAMS) offers a data-driven and tech-enabled environment with its ability to generate individual and group test results and statistical reports, enable profiling

and analysis of training performance at various levels, and provide a predictive model of the training population to introduce early intervention regimes to optimise responders' performance.

CONCLUSION

Beyond meeting the rapidly evolving training needs of the SCDF, the next-generation training infrastructure of CDA is also envisioned to be a platform for collaboration and a focal point for knowledge creation through scientific research and innovation. SCDF welcomes partnerships with other emergency response agencies, institutes of higher learning, and other like-minded entities to join its endeavour to continually improve the safety, health, and performance of emergency responders. The establishment of ExCEL will enable the SCDF to use evidence-based research to develop new training paradigms and enhance the overall operational readiness of the Home Team.



ABOUT THE AUTHORS



Hasan Kuddoos

currently holds the appointment of Commander Marina Bay Fire Station. Prior to his current posting, Hasan was the Principal Responder Resilience & Systems Officer with the Responders' Performance Centre at Civil Defence Academy. Hasan has been actively involved in various innovation and research projects to improve training efficacy among trainees. Some of his notable projects include a profiling study on individuals' heat stress index in a bid to improve heat endurance related to training. projects to improve training efficacy among trainees. Some of his notable projects include a profiling study on individuals' heat stress index in a bid to improve heat endurance related to training.



Melissa Choo

is currently a Senior Staff Officer in Organisation Review at the Planning & Organisation Department of SCDF. She led the conduct and coordination of the SCDF Workplan Seminar 2022 which unveiled numerous transformation projects and included the inaugural showcase of the ExCEL.

REFERENCES

Trinh, C. M., & Matthew, T. (2019, March). *Predicting VO2max from 1- and 1.5-mile Runs*. Texas Health Resources.

DEVELOPING FUTURE-READY HOME TEAM OFFICERS THROUGH DATA ANALYTICS UPSKILLING

Tanny Ng, Rachelle He & Nicole Lee

Centre for Home Team Skills Transformation, Home Team Academy

ABSTRACT

To deliver improved public services to the people, Singapore's public sector has been investing in the digitalisation of government services as well as the deployment of new technologies. Since 2018, the Home Team Academy (HTA) and the Ministry of Home Affairs headquarters has been working closely to implement a mandatory training intervention to equip all Home Team officers with data analytics knowledge, and the skill and competencies to analyse data and make informed recommendations to advance the Home Team's performance. To ensure effectiveness of training intervention efforts, the HTA Evaluation Approach is used to conduct post course impact training evaluation to assess data analytics skills acquisition and application in the Home Team. This article documents HTA's journey in developing future-ready Home Team officers through mandatory training interventions on data analytics, as well as efforts in conducting post course impact training evaluation to assess the training. The article concludes by sharing HTA's efforts and plans to further push training and learning transformation plans to enable a more effective and future-ready Home Team.

A CITIZEN-CENTRIC PUBLIC SERVICE

The Singapore Public Service has been using new tools and technologies to change the way public officers work and operate, redesigning work processes for improved efficiency and productivity, and building diverse capabilities to serve Singaporeans better. To be more citizen-centricity, the public sector uses technology as a force multiplier to improve operational and service processes, so that government services and resources are increasingly integrated, digitalised and personalised to meet citizens' needs. For example, the LifeSG app provides a one-stop suite of services across every citizen's key life events from childbirth to marriage, to retirement and eligibility for government benefits. Using Singpass as the trusted digital identity makes transacting with government and businesses faster and easier. When COVID-19 became a global pandemic, the TraceTogether app, developed within months of Singapore's first COVID-imported case, played a key role in helping the nation contain the spread of the virus through contact tracing.

Within the Home Team, technology, particularly in data analytics and automation, has enabled departments to operate more efficiently and effectively. For example, since 2013, data science has changed how the Singapore Civil Defence Force operates. By reviewing factors such as patient's medical condition, the emergency medical service resources available in an area, and traffic patterns, the SCDF can ensure critical medical cases receive medical attention at a faster rate (Tan, 2018).

DEVELOPING THE FUTURE-READY HOME TEAM OFFICER

The Home Team Transformation efforts, which began in earnest in 2015 to prepare for challenges arising from increasing demands and limited manpower, aims to optimise resources for maximum impact, synergy and effectiveness. This has, not surprisingly, meant an increased pace of adoption of technology to enhance digitalisation and data analytics capabilities across the Home Team for operational efficiency, and to empower and strengthen community partnerships. A key requirement is to develop future-ready officers

equipped with the required competencies to meet future challenges. This is a vision that has been strongly articulated and reiterated by Home Team leaders over the years (see box).

Minister for Home Affairs K Shanmugam on the Future-Ready One Home Team (2017):

“We have to use more technology and data across the Home Team. For example, Police will issue every frontline Police officer with a smartphone. This will allow our Police officers to be updated with timely and relevant information on-the-go, and as they arrive at their destination, they can pull out and look at a variety of data that is relevant. It will help provide our officers with more situational awareness.

ICA for example, has started to collect iris images. At the checkpoints, we will use multi-modal biometrics. That will help us in our identity verification, and at the same time we will increase the number of automatic clearance counters.

CNB will use data analytics to conduct risk assessments of every drug supervisee so that we do not need to look at all the supervisees in the same way. We will watch higher-risk drug supervisees more closely, and some others with lower-risk will require a lower level of intervention. That will free up our CNB officers to focus on other critical tasks. That is a snapshot of how we are going to bring in technology together with an evidence-based approach.”

A workforce that is digitally conversant and a smart user of data is able to make sense of data, think, and act in innovative ways to generate new solutions on the ground. Data in itself is, however, rarely meaningful until it is processed and analysed. As technology expert Peter Sondergaard, once put it, “Information is the oil of the 21st century, and analytics is the combustion engine” (Business Wire, 2011).

The Ministry of Home Affairs (MHA) thus adopts an aggressive approach in upgrading the digital and data analytics capabilities of all its officers. In line with the Public Service Division’s refreshed Core Competency Framework for all Public Service

officers – which lists data analytics as one of the core competencies – MHA has made it mandatory for all Home Team officers to be equipped with data analytics competencies so they can analyse data and make data-informed recommendations. By 2025, the Home Team intends to become significantly more data driven, and future-ready to meet evolving challenges.

TRAINING AND LEARNING AS KEY ENABLER FOR UPSKILLING

Training and learning (T&L) is a key enabler for Home Team leaders and officers to discharge their duties purposefully and effectively to achieve mission success. As the corporate university of the Home Team, the Home Team Academy (HTA) plays a pivotal role in developing skilled and future-ready Home Team officers. HTA develops Home Team leaders, civilian officers, and trainers through foundation training, leadership programmes, and skills transformation to produce skilled and trusted Home Team officers. HTA partners leading T&L institutions to develop quality programmes and collaborates with Home Team Departments to co-develop and implement T&L initiatives to develop Home Team officers.

The [Centre for Home Team Skills Transformation](#) in HTA supports MHA in driving the overall continuing education and training strategy as well as implementing training programmes to equip Home Team officers with a robust set of strategic and transformational cross-cutting skills and knowledge to meet MHA’s needs. The aim is to prepare Home Team officers to meet future challenges with data analytics, design thinking, cyber security, behavioural insights, collaboration and engagement, and technology literacy competencies.

The Centre recognises 4 levels of competence as illustrated in Figure 1:

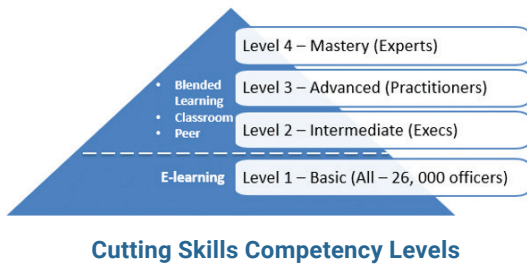
- a. Level 1 (Basic) for all Home Team officers who are expected to have some knowledge of the skillsets, the terminology, and concepts. Due to the large volume of officers to train and the need to train officers within a short time span, the key training modality is eLearning.
- b. Level 2 (Intermediate) for Executives who are required to use the skillset at their present job or in future without much supervision.
- c. Level 3 (Advanced) for Practitioners who need

to have the knowledge and experience to carry out complex tasks confidently and consistently and may need to supervise others.

- d. Level 4 (Mastery) for Experts.

The key modalities for Levels 2 to 4 are blended learning, which comprises online and physical classroom and peer learning.

Figure 1. Strategic and Transformational Cross-



IMPLEMENTING DATA ANALYTICS TRAINING FOR THE HOME TEAM

Targeted and Tiered Training Approach

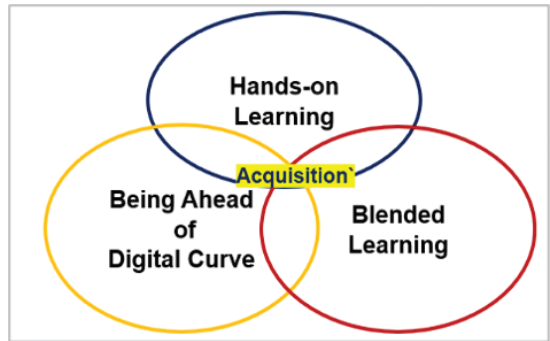
The Home Team officer of the future is envisioned to be a digitally conversant, technologically savvy and smart data user with strong security acumen and excellent soft skills to engage and develop deep partnerships with stakeholders such as local communities, businesses and international partners. As Home Team officers increasingly access and synthesise data from multiple sources, data analytics training enables them to distil meaningful patterns in data and generate useful insights for better performance at work.

In 2018, HTA started rolling out data analytics training for Home Team officers. To do so, HTA adopts three key principles, as shown in Figure 2, to enable digitalisation skills acquisition in the Home Team. First, mandating training for all Home Team officers to signal the importance of upskilling so officers can be ahead of the digital curve. Second, delivering training through a blended learning approach, and thirdly, including hands-on learning to achieve the best learning outcomes.

Data analytics training is delivered for two target groups, from staff officer level to Commanders/Directors.

At basic Level 1, HTA trains about 26,000 Home Team officers with different learners’ profiles and

Figure 2. Key Principles Enabling Digitalisation Skills Acquisition in the Home Team



background, so that they all gain at least a basic understanding of data analytics. This is done primarily through e-learning, MHA’s data analytics broadcast, and bite-sized online learning content to create awareness, ignite interest, and facilitate self-directed learning. Data analytics e-learning modules, such as the Data Literacy ePrimer and the Data Analytics Awareness e-course, are mandatory for all officers. The e-learning modules equip officers with a broad basic understanding of data analytics on various aspects from the importance of visual analytics and its impact on collecting good quality data and building dashboards, to understanding the way algorithms and techniques work behind data science and artificial intelligence (AI); knowing the applications, strengths and weaknesses of data science and AI; and sharpening problem statements to be solvable through data science and AI techniques and applications. As these modules are easily accessible through their mobile devices, officers can complete the modules on the go at their own time and convenience.

At Level 2 for intermediate learners who need to apply data analytics skills at work, training is delivered through a blended learning approach – virtual and/or in-person physical classroom –over a 1 to 2.5 days training session, depending on their job profile. Through the training, officers gain a deeper understanding and better appreciation of data analytics concepts and principles such as the different types of data analysis, i.e. descriptive, prescriptive, predictive, qualitative and quantitative analysis. The hands-on practicum session in the training equips officers with the ability to apply key tools and methodologies used in analytical decision-making, data visualisation, and to define and critique

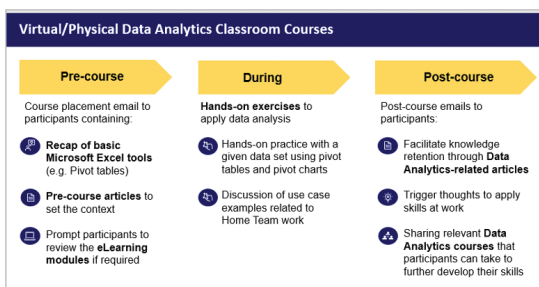
a well-scoped problem statement solvable through a data science approach. The hands-on exercises in the curriculum give officers the opportunity to apply the analytical skills and techniques learnt in case examples related to the Home Team. HTA also circulates relevant articles to facilitate continuous learning for Home Team officers and promote Community of Practice activities related to data analytics to past and new course participants.

At Level 3 for practitioners and Level 4 for subject matter experts, specialised and targeted training are planned and managed by the respective MHQ Divisions and HT departments. HTA works closely with the rest of the HT to strengthen HT organisation capability to keep Singapore safe and secure.

Touchpoints with Course Participants

HTA engages data analytics course participants through three key touchpoints of a virtual or physical in-person classroom training: pre-course, during, and post-course, as detailed in Figure 3. In the pre-course phase, participants receive a course placement email with pre-course articles, refresher tips on basic Microsoft Excel tools such as pivot tables, and a prompt to complete and review the mandatory data analytics eLearning modules. During the course, participants will have several hands-on exercises and Home Team-related case examples to apply the data analytics skills and knowledge learnt. After completing the courses, HTA continues to engage the participants with a series of initiatives via email. This includes circulating relevant articles to facilitate knowledge retention; using Behavioural Insights techniques to nudge self-directed learning by sharing up-and-coming data analytics-related courses offered by Civil Service College and eLearning courses available on LEARN app; as well as prompting signups

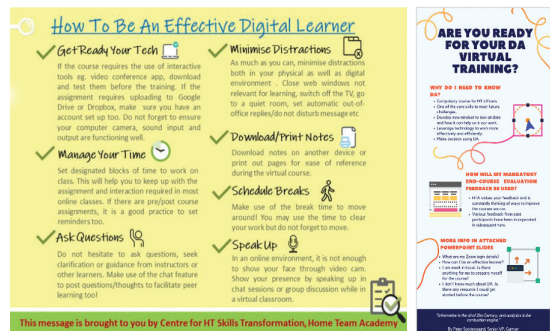
Figure 3. HTA Touchpoints with Data Analytics Course Participants Ensuring Data Analytics Training Continuity



to GovTech mailing list for a host of data science related workshops and activities through the Data Science Connect Spark Newsletter that connects data science enthusiasts and practitioners across Whole of Government. To provide continuous outreach to Level 1 (Basic) learners, HTA also partners MHA headquarters and Home Team Science & Technology Agency (HTX) to curate and broadcast, for a month, bite-sized online content on Workplace by Facebook.

When the COVID-19 pandemic disrupted and halted physical in-person activities, HTA swiftly pivoted its data analytics training and learning approaches, from physical in-person classroom to fully virtual modality via virtual conferencing platforms. This swift transition was possible only because of HTA's strong relationship with training partners to optimise training delivery. As learning virtually may be daunting and unfamiliar to some, HTA also designed and disseminated simple but informative infographics detailing virtual learning tips to better prepare participants for virtual learning, as illustrated in Figure 4. Since the transition to blended learning modalities, feedback from course participants has been positive and ratings have been comparable to physical in-person course runs meeting at least 90% and above in course satisfaction.

Figure 4. Examples of infographics designed by HTA on virtual learning tips to better prepare participants for virtual learning



Recognising that online and blended learning modalities will become the new normal, HTA has established an Online Learning Asset Portal available on the HTA intranet for all Home Team officers and trainers to keep abreast of best practices, tips and information on how to learn and train more effectively through different modalities such as microlearning, mobile learning, eLearning and blended learning.

Navigating Training Constraints and Challenges

Delivering the training in a timely manner is crucial, but also a challenge. As officers come from diverse background and have varying training and learning needs, HTA constantly experiments with ways to curate right-sized basic-level programmes that are useful and relevant for both the Home Team Departments and individual officers. Home Team operations are also rigorous and constantly at high tempo. When rolling out the training programmes, it is important to strike a balance between training needs and operational demands, particularly during key national events where ground deployment will be tight, on top of school holidays and festive seasons.

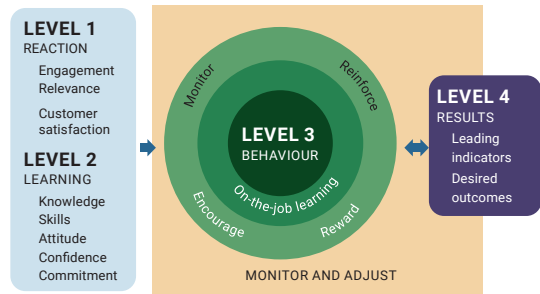
HTA is continuously working toward better positioning continuous learning as second nature to Home Team officers. For example, HTA urges training coordinators in each Home Team Department to prioritise sending supervisors to attend the course first to create awareness at the supervisors' level. The team also customises content for different learning styles, and identifies ambassadors to advocate new ways of learning.

RIGOROUS TRAINING EVALUATION FOR DATA ANALYTICS

Training evaluation is fundamental to achieving desired learning outcomes and offers opportunities to refine and sharpen training curriculum and delivery for maximum results. HTA has in place a standardised Evaluation Approach that adopts the New World Kirkpatrick Model, as shown in Figure 5, for our programme evaluation process. Levels 1 and 2 Evaluation are conducted for all programmes conducted by HTA. Through the use of simple, easy-to-administer end-of-course/programme evaluation forms, these levels measure the degree to which participants find the training programmes engaging and the degree to which they are able to acquire knowledge, skills, attitudes, confidence and commitment due to their participation in the programmes. Course administrators regularly sit in and observe the training sessions to better experience the training delivery by the trainers and observe the responses of participants. End-of-course evaluation is also administered for each course run of the data analytics training, where rigorous analysis of the qualitative and quantitative data is conducted on a regular and timely basis. This allows HTA to work with the Civil Service College and the trainers to review the feedback and incorporate participants' suggestions to

swiftly fine-tune the training programme and delivery for subsequent runs. This helps to optimise learning outcomes. HTA also provides opportunities for feedback by inviting staff to surface any issues related to the course through the post-course email. This approach has been useful given the scale and volume of data analytics for the Home Team.

Figure 5: The New World Kirkpatrick Model of Training Evaluation



© 2023 Kirkpatrick Partners, LLC. All Rights Reserved.

However, such evaluation is pegged at the first two levels of the Kirkpatrick Model which focus on measuring the degree participants acquire the intended knowledge, skills and attitudes during training. Following the HTA Evaluation Approach, Kirkpatrick Levels 3 and 4 evaluation are only done at the discretion of programme owners because not every training course requires an in-depth evaluation that measures critical behaviours performed by learners on the job following the training and subsequent reinforcement.

Data Analytics Post-Course Impact Study

Given that the course is mandatory to prepare officers' future-readiness, HTA recognised the timeliness of conducting a post-course impact study when half of the targeted pool in the Home Team had been trained. In 2020, HTA conducted a post-course impact study pegged at Kirkpatrick Level 3 to better assess the effectiveness of the data analytics training, skills acquisition and application across the Home Team, and to ensure participants were truly impacted by the learning and were applying what they learnt. The HTA Evaluation Approach was also referenced in the conduct of the post-course impact study, particularly on the framing of questions. The HTA approach provides an up-to-date, systematic and consistent framework for training evaluation that incorporates different training modalities. The evaluation questions are benchmarked against industry norms and are

sequentially placed and organised to distil a more accurate evaluation and feedback from participants.

The impact study identified officers across the Home Team Departments who had completed the data analytics training three to six months earlier. Additional efforts were made to engage their immediate supervisors as they play a critical role in facilitating and supporting officers' application of newly acquired skills at work.

Improved Work Performance and Greater Confidence in Applying Data Analytics

The majority of the respondents found the training to be useful and well delivered by competent and engaging trainers. The curriculum had good topics coverage on data visualisation, analytics and analysing data using pivot tables and Excel tools. This was largely evidenced by positive end-of-course feedback that the course was well conducted, with compliments to the trainers for being knowledgeable, encouraging, and engaging and delivering the course effectively. Respondents also commented that the course provided them with greater awareness, understanding and appreciation of data analytics application not just at work but in everyday life with many real-life case examples provided by the trainers.

Respondents said that they had become not only more aware of the value of data analytics and its impact on decision making, but they also reported greater confidence in immediately applying data analytics at work. They observed that such applications helped them to improve their work efficiency and performance. Similarly, supervisors observed that their staff were able to better perform data analytics tasks without seeking assistance as compared to pre-training, and some were even able to teach others. Notably, some of the respondents also shared their new knowledge with their colleagues and were able to guide them on data analytics application. To encourage the sharing and to help with knowledge retention, HTA has been curating and sending relevant data analytics articles and intermediate course materials to all course participants after completion of their training.

Among those who did not report positive changes after completing the course were participants who felt their work gave them little scope to apply or share their newly acquired data analytics skills. They indicated that more opportunities for practice and application would

help promote transfer of the knowledge. In this regard, HTA worked with HTX to promote case examples of data analytics at work in the Home Team, to help officers understand how and where data analytics can be applied in their operating environment. Across the Home Team Departments, data analytics have been used in policing, counter-terrorism, fire-fighting, border operations, rehabilitation, corrections and drug control, where insights from large and varied droves of data sources are drawn to make informed decisions and respond more efficiently to incidents.

Taking Ownership of Learning with Supervisors' Support

Another positive training outcome achieved was the response from the majority indicating their keen interest to deepen their data analytics competency by taking ownership of their own learning. Many have become more aware and appreciative of the usefulness and magnitude of the impact that data analytics plays in problem resolution, as well as the powerful insights that can be inferred from the voluminous data around them. They want to adopt the data analytics and visualisation skills in their work presentation or problem resolution and embark on self-directed learning. Some are inclined to participate in project work that require the application of data analytics skills, while others will consult their supervisors for advice and support to deepen the competency. The impact study also revealed that supervisors' support in helping staff to identify opportunities, be it within job scope or cross-collaboration projects, is key to facilitating data analytics skills application at work. Supervisors indicated in the study their commitment to helping their staff further deepen their competency in data analytics wherever applicable, through generating new opportunities and work areas for staff to apply their learning, illustrate the usefulness and relevance of applying data analytics and demonstrating how the newly acquired skills can be applied.

ACHIEVING DATA ANALYTICS TRAINING OUTCOMES AS ONE HOME TEAM

Since the launch of the data analytics training in 2018, HTA has consistently achieved more than 90% ratings in training satisfaction over the five years. It takes a One Home Team approach to achieve these outstanding outcomes. To ensure effective learning takes place and desired training outcomes are achieved, HTA works very closely with MHA headquarters to identify

relevant courses, other Home Team departments on training implementation, evaluation and review, and subject matter experts from HTX on content development. On training delivery, HTA works with external training providers, e.g., the Civil Service College, to curate and engineer the best learning experiences for Home Team officers.

HTA recognises the need for continuous engagement with officers on the importance of acquiring cross-cutting skills (e.g. data analytics in this case) within the Home Team. Moving forward, HTA will enhance communication and publicity efforts to raise more awareness in facilitating these skills acquisition with the right learning attitude and mindset.

This post-course impact study provided holistic insights on the usefulness of the data analytics training in increasing data analytics competency across the Home Team and the key factors for successful training interventions. It also revealed training constraints. These insights allow HTA to make data-informed recommendations to better facilitate the initiation of data analytics application at work and the acquisition of competencies.

Applications of Data Analytics in Home Team Academy

In its journey advancing towards a [Smart Campus 2025](#), HTA will be leveraging more technology and digitalisation to build HTA's internal and external-serving capabilities. In June 2022, HTA collaborated with HTX in the development of dashboards for training safety, estate management and training and learning. Specifically in the area of T&L, HTA will be establishing a data dashboard for end-of-course and post-programme evaluations. This will help HTA actualise the [Centre of Excellence \(CoE\) in Evaluation and Assessment](#), where the evaluation and assessment systems in HTA Centres and eventually across the whole of the Home Team will be made robust, valid, and reliable.

FUTURE OF LEARNING IN THE HOME TEAM

The rate of technology disruption has significantly increased in recent years. Thus, it is important for HTA to champion digital upskilling and nudge Home Team officers to proactively acquire new

skillsets beyond immediate utilisation in their current work roles.

Upskilling Home Team officers with data analytics competency is only the beginning. A good data analytics foundation charts the path towards the ability to leverage more complicated and sophisticated digital tools and software, such as robotic process automation, machine learning, coding and artificial intelligence (AI). To meet the demands of the future of work, HTA will be refining the future of learning in the Home Team by helping Home Team officers gain knowledge, capability and confidence in the use of technology tools and applications.

At the same time, in the journey to upskill all Home Team officers in digital skills, each Home Team department is customising its own digital training plans based on its own needs. Some of the new digital skills that will form the overarching training framework include coding, application development, cloud technology, Internet of Things, robotic process automation, AI and machine learning. HTA will be supporting these digital upskilling plans through good and effective T&L strategies and initiatives.

Recognising that Home Team officers will have shorter and more compact learning cycles, HTA will also be setting up a [Centre of Excellence in Online Learning](#) to build online learning capabilities in the Home Team and strengthen the rigour of online learning applications through the use of technology. Its work will not be limited to systems on creating access to training online but will also involve cultivating online learning habits in Home Team officers to be self-directed in gaining new skillsets, as well as future-proof HT trainers by equipping them with competencies and knowledge on digital tools to navigate the diverse online learning modalities.

As HTA strives towards becoming a digitally empowered and future-ready Corporate University of the Home Team, it will continuously strengthen the T&L ecosystem that maximises collaboration, shares best practices and delivers relevant and timely training to develop future-ready Home Team officers.

ABOUT THE AUTHORS



Tanny Ng

is Director of the Centre for Home Team Skills Transformation in the Home Team Academy. She leads the team driving Home Team-wide initiatives relating to strategic and transformational cross-cutting skills and continuous education training with programme accreditation.



Rachelle He

is a Senior Executive with the Centre for Home Team Skills Transformation, Cross-Cutting Skills Branch, in the Home Team Academy. Her job scope includes training evaluation of cross-cutting skills, executing behavioural insights projects to develop and apply behavioural insights tools in nudging data analytics upskilling across the Home Team, as well as the conceptualising and planning of initiatives to drive the importance of cross-cutting skills in the Home Team.



Nicole Lee

is an Executive on temporary contract with the Centre for Home Team Skills Transformation, Cross-Cutting Skills Branch, in the Home Team Academy. Her job scope includes supporting the Cross-Cutting Skills team in administering training evaluation work and behavioural insights project as well as conducting cross-cutting skills training needs analysis research for the team.

REFERENCES

Ang, H. S., & Soon, S. (2021). Transformation in the Singapore Public Service: Emerging stronger from the pandemic. *Civil Service College*. <https://www.csc.gov.sg/articles/transformation-in-the-singapore-public-service-emerging-stronger-from-the-pandemic>

Business Wire. (2011). *Gartner says worldwide enterprise IT spending to reach \$2.7 trillion in 2012*. <https://www.businesswire.com/news/home/20111017006470/en/Gartner-Says-Worldwide-Enterprise-IT-Spending-to-Reach-2.7-Trillion-in-2012>Co, C. (2020). Emerging Stronger Taskforce will identify global risks, seize economic opportunities for Singapore: Desmond Lee. *CNA*. <https://www.channelnewsasia.com/singapore/emerging-stronger-taskforce-covid-19-economy-desmond-lee-657016>

Eggers, W. D., Boyd, J., Knight, J., Cooper, S., & Kishnani, P. K. (2022). How government can deliver streamlined life event experiences. *Deloitte Singapore*. <https://www2.deloitte.com/xe/en/insights/industry/public-sector/citizen-centric-government.html>

Home Team Science and Technology Agency. (2022). *Data science & AI*. <https://www.htx.gov.sg/what-we-do/our-expertise/data-science-ai>

Kirkpatrick, J.D., & Kirkpatrick, W.K. (2016). *Kirkpatrick's Four Levels of Training Evaluation*. Alexandria, VA: ATD Press.

Lee, H. L. (2013). Speech by Prime Minister Lee Hsien Loong at Public Service Leadership Advance on 30 Sep 2013. <https://www.pmo.gov.sg/Newsroom/speech-prime-minister-lee-hsien-loong-public-service-leadership-advance-30-sep-2013>

Lee, H. L. (2014). PM Lee Hsien Loong at the Smart Nation Launch. <https://www.pmo.gov.sg/Newsroom/transcript-prime-minister-lee-hsien-loongs-speech-smart-nation-launch-24-november>Ministry of Home Affairs. (2018). *Home Team Journal Issue No. 7*. <https://www.mha.gov.sg/hta/publications/publications-content/publications/home-team-journal-issue-no.-7>

Ministry of Home Affairs. (2022). *Transforming the Home Team*. <https://www.mha.gov.sg/what-we-do/transforming-the-home-team>

Ng, C. K. (2019). Digital government, Smart Nation: Pursuing Singapore's tech imperative. *GovTech Singapore*. <https://www.tech.gov.sg/media/technews/digital-government-smart-nation-pursuing%20singapore-tech-imperative>

Public Service Division. (2015). *Building a public service ready for the future*. <https://www.psd.gov.sg/heartofpublicservice/our-institutions/building-a-public-service-ready-for-the-future/>

Saminathan, M. a/p., & Suaib, N. M. (2021). Training evaluation models for skill-based E-learning system: A systematic literature review. *International Journal of Innovative Computing*, 11(2), 61-65. <https://doi.org/10.11113.ijic.v11n2.323>

Shanmugam, K. (2017a). Home Team Promotion Ceremony 2017 – Speech by Mr K Shanmugam, Minister for Home Affairs and Minister for Law. <https://www.mha.gov.sg/mediaroom/speeches/home-team-promotion-ceremony-2017---speech-by-mr-k-shanmugam-minister-for-home-affairs-and-minister-for-law/>

Shanmugam, K. (2017b). *Message from Minister K Shanmugam to the Home Team*. <https://www.police.gov.sg/media-room/features/message-from-minister-k-shanmugam-to-the-home-team>

Singapore Management University, 2022. *The Singapore TraceTogether story for COVID-19 contact tracing*. <https://news.smu.edu.sg/news/2022/04/08/singapore-tracetgether-story-covid-19-contact-tracing>

Tan, M. (2018). Data science in the Home Team. *Ministry of Home Affairs*. <https://www.mha.gov.sg/home-team-news/story/detail/data-science-in-the-home-team/>

Yip, L. (2020). Speech by Mr Leo Yip, Head, Civil Service at the 2020 Annual Public Service Leadership Dinner. <https://www.psd.gov.sg/press-room/speeches/speech-by-mr-leo-yip--head--civil-service-at-the-2020-annual-public-service-leadership-dinner>

UNDERSTANDING ONLINE HATE SPEECH IN SINGAPORE: A BEHAVIOURAL SCIENCES AND PSYCHOLOGICAL PERSPECTIVE

Hong Jingmin, Nur Aisyah Abdul Rahman, Gabriel Ong,
Shamala Gopalakrishnan & Majeed Khader
Home Team Psychology Division, Ministry of Home Affairs, Singapore

ABSTRACT

There is growing evidence that online hate speech can promote prejudice and intolerance, deepen social divides, and even incite offline violence. However, little is known about the prevalence and spread of hate speech on social media, especially in the Singapore context. Using cutting-edge deep learning techniques for Natural Language Processing (NLP) tasks, this study collected 233,997 Facebook posts and comments to identify the commonly targeted out-groups and intensities of hate speech. Our results identified the common targets of hate speech, which include people of other nationalities, people of other races, people of other religions, the LGBT community, people of other socio-economic status, people with differing political ideology, and people in or associated with the government. We also categorised online posts and comments into eight levels of hate intensity, and found a significant but small relationship between the hate intensities of posts and comments. Drawing from a behavioural sciences perspective, implications for policy makers, researchers, and practitioners are discussed.

WHAT IS HATE SPEECH?

The term “hate speech” is easier to grasp as a concept than it is to define. Depending on the context, hate speech can be defined in various ways based on its content, the intrinsic properties (i.e., the types of words used, such as slurs), the harm caused, and the undermining of the targeted group’s dignity (Anderson & Barnes, 2022). Consider the following examples: “*There is no place for sensitive feminists here*” and “*I will kill you, feminist bitch*”. Some people may consider both to be hate speech, while others may consider only the latter as hate speech due to the clear threat of harm expressed. In Singapore, there is no official definition of hate speech, but under the Penal Code, “speech and other verbal communications that could lead to violence, disobedience to the law or a breach of the peace” will be prohibited (Sedition (Repeal) Bill 2021 (23), cl 4).

The definition of hate speech may also differ in terms of the characteristics protected from being the target

of hate. For instance, the Broadcasting Complaints Commission of South Africa (2017) defines hate speech as “any utterance that advocates hatred that is based on race, ethnicity, gender or religion, and which constitutes incitement to cause harm”, while the Council of Europe’s Committee of Ministers (1997) adopts a more inclusive perspective by considering hate speech as “all forms of expression which spread, incite, promote or justify racial hatred, xenophobia, anti-Semitism or other forms of hatred based on intolerance, including intolerance expressed by aggressive nationalism and ethnocentrism, discrimination and hostility towards minorities, migrants and people of immigrant origin”.

As there is no standardised legal or academic definition of hate speech, the approach to monitoring and intervening against hate speech varies across countries and organisations. For the purpose of this study, hate speech is defined as “any form of speech that directly attacks or promotes hate towards a group or an individual member, based on

their actual or perceived aspects of identity, such as ethnicity, religion, and sexual orientation” (Yin & Zubiaga, 2021). We use a broad definition that captures a wide range of expression and allows for a wide variety of actionable use (Quinn, 2019), such as monitoring inter-group tensions across areas of concern; triaging the distribution of human, material, and financial resources; performing long-term analysis on underlying causes; and applying predictive results to inform intervention efforts. Critically, this definition of hate speech is inclusive of the broadest range of protected characteristics, including but not limiting to race, ethnicity, religion, nationality, political opinion, sex, and sexual orientation, as suggested by ARTICLE 19¹ (2015), an international human rights organisation.

WHY STUDY HATE SPEECH?

“Hate speech desensitises individuals. It normalises behaviour which is otherwise unacceptable. It stokes anger and fear and provides a surge of stress hormones.”

K Shanmugam, Minister for Home Affairs and Minister for Law, 2019

Historically, hate speech has been associated with offline violent actions. A 2018 study found that anti-refugee hate crimes in Germany increased disproportionately in areas with higher Facebook usage during periods of high anti-refugee sentiments online, suggesting a transmission of online hate speech into offline violent hate crimes (Müller & Schwarz, 2020). In the United States, the Boogaloo movement, a loosely organised far-right anti-government extremist movement, originated from an anti-establishment online meme promoting civil war and gun rights, but has since evolved into an offline decentralised extremist militia. Supporters of the Boogaloo movement have been involved in various extremist attacks, such as the US Capitol riots on 6 January 2021 (Hatewatch, 2021). Closer to home, the Myanmar military has been accused of using Facebook to spread anti-Rohingya propaganda and incite an ethnic cleansing campaign (Mozur, 2018).

Hate speech towards the Muslim Rohingyas include derogatory terms like “Bengalis” and dehumanising references like “non-human kalar dogs”, “maggots”, and “rapists” (Stecklow, 2018). In particular, Wirathu Ashin, the leader of the 969 Movement, has called mosques “enemy bases”, and has encouraged Buddhists to boycott Muslim businesses and shun interfaith marriages (Marshall, 2013).

International law has traditionally prohibited hate speech that explicitly incites discrimination, hostility, and violence offline (ARTICLE 19, 2015). This type of hate speech is particularly concerning as it is explicitly and deliberately aimed at triggering discrimination, hostility, and violence, which may lead to or include terrorism or (hate) crimes (United Nations, n.d.). In addition, it is critical to highlight that lower levels of hate speech are also of concern to the safety and security of the nation, as repeated exposure of hateful and discriminatory attitudes can normalise hateful behaviours and escalate into higher levels of hate (Bahador et al., 2019). Experts have also warned that hate speech may polarise public opinion and hurt political discourse (Siegel, 2020). To seriously fight hate speech and its violent and destabilising consequences, it is important to consider its earliest manifestations to prevent and mitigate escalation (Bahador et al., 2019).

Types Of Hate Speech

With many studies that explore the identification of hate speech on online platforms, the classification tends to be binary – hate-speech, and non-hate speech (e.g., Corazza et al., 2020) – or up to three levels – hate-speech, non-hate speech, or offensive speech (e.g., Watanabe et al., 2018). However, hate speech can vary widely in terms of intensity and severity. For example, the examples previously cited – “There is no place for sensitive feminists here” and “I will kill you, feminist bitch” – both reflect discriminatory and hateful sentiments towards “feminists”, but a distinction should be made as the latter expresses a clear threat of physical harm and requires more legal intervention and response.

¹ARTICLE 19 (<https://www.article19.org/>) is an international human rights organisation, with its name inspired by Article 19 of the Universal Declaration of Human Rights. It provides legal analyses of national laws relating to free expression and shapes international standards on the right to freedom of expression and information.

In recognition of such variances in hate speech, ARTICLE 19 (2015) identifies three types of hate speech:

- 1) hate speech that must be prohibited;
- 2) hate speech that may be prohibited; and
- 3) lawful hate speech.

As shown in Figure 1, the three subcategories are ordered in increasing severity and require different responses. At its highest, hate speech that must be prohibited includes the most severe forms that intend to incite exceptional and irreversible harms. This includes incitement of discrimination, hostility, violence, or genocide, as well as other violations of international law.

In cases where the speaker does not seek to incite actions against the target out-group, such less severe forms of hate speech may be restricted to protect the rights of others, or in the interest of national security. Finally, the base of the pyramid consists of lawful hate speech that should be protected from restriction, but nevertheless raises concern in terms of intolerance and discrimination (ARTICLE 19, 2015).

Similarly, Bahador and colleagues (2019) believe that it is important to acknowledge the distinguishable variations of intensities of hate speech. They have developed a 6-point hate speech intensity scale, based on extensive content analysis of US news

Figure 1. Hate Speech Pyramid (ARTICLE 19, 2015)

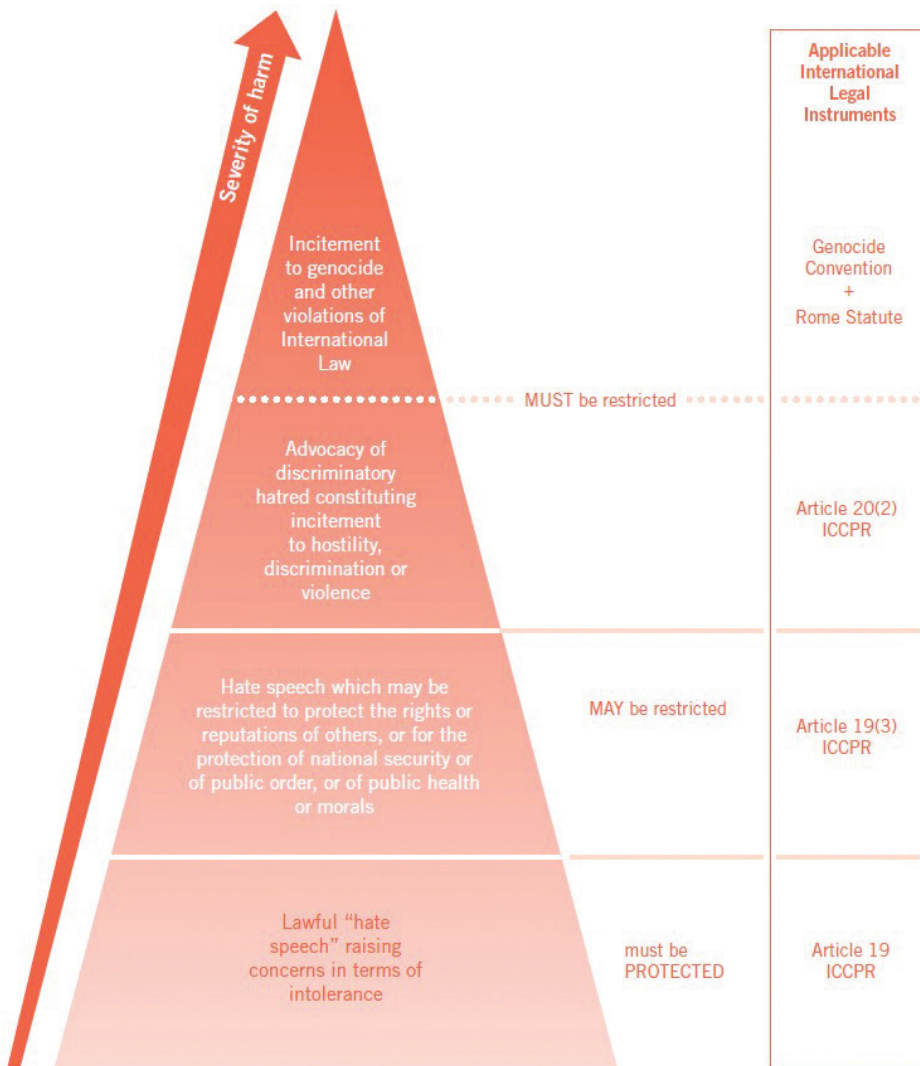








Figure 2. Bahador et al., (2019) Hate-Speech Intensity Scale

Color	Title	Description	Examples
	6. Death	Rhetoric includes literal killing by group. Responses include the literal death/elimination of a group.	Killed, annihilate, destroy
	5. Violence	Rhetoric includes infliction of physical harm or metaphoric/ aspirational physical harm or death. Responses include calls for literal violence or metaphoric/aspirational physical harm or death.	Punched, raped, starved, torturing, mugging
	4. Demonizing and Dehumanizing	Rhetoric includes subhuman and superhuman characteristics. There are no responses for #4.	Rat, monkey, Nazi, demon, cancer, monster
	3. Negative Character	Rhetoric includes nonviolent characterizations and insults. There are no responses for #3.	Stupid, thief, aggressor, fake, crazy
	2. Negative Actions	Rhetoric includes negative nonviolent actions associated with the group. Responses include nonviolent actions including metaphors.	Threatened, stole, outrageous act, poor treatment, alienate
	1. Disagreement	Rhetoric includes disagreeing at the idea/belief level. Responses include challenging claims, ideas, beliefs, or trying to change their view.	False, incorrect, wrong, challenge, persuade, change minds

media and review of the academic literature on hate speech and related topics (see Figure 2). At each level, Bahador et al., (2019) distinguish between the negative words or phrases associated with the target out-group (which they refer to as rhetoric) and the proposed actions that the in-group should take against the out-group (which they refer to as response). Hate speech can range from disagreements directed at an out-group's values and beliefs, to calls for lethal violence such as the death or elimination of a target out-group.

Based on the reasons outlined above, this study adopts a more nuanced approach of examining hate speech based on its intensity level, rather than collapsing all types of hate speech into a single category. This is useful as different intensities of hate speech may signify different severities of impact, and correspondingly call for different responses and management strategies.

OBJECTIVES OF STUDY

By using a psychological and behavioural sciences approach and applying data science methods, this exploratory study seeks to examine the prevalence and spread of hate speech on Facebook, which has been found to be second most popular social media platform used in Singapore, after WhatsApp (Statista, 2022). Three research questions are of interest in this study:

1. What are the prevalent targets of online hate speech?
2. What are the prevalent intensities of online hate speech?
3. How does the intensity of the hate post influence the intensity of subsequent hate comments?

METHODOLOGY

Data Collection

Data was collected from various publicly accessible groups and pages known to discuss controversial views on Facebook. This included pages and groups that aimed to discuss specific issues such as the now defunct Abolish CECA group page, where members expressed grievances they associated with the Singapore-India Comprehensive Economic Cooperation Agreement (CECA)². In total, 233,997 online posts and comments were collected from the last 5 years, from 12 October 2016 to 30 September 2021, to assess recent public sentiments.

Data Analysis

The data analysis approach for the current study is largely similar to that of other studies that analyse data from social media in various contexts (e.g., Ayo et al., 2020; Ayoub et al., 2021; Chen et al., 2022; Singh et al., 2021).

Text pre-processing

Posts and comments were pre-processed by removing null and repeated entries, removing stop-words and non-alphanumeric characters (e.g., emojis, URLs, hashtags), and lower-casing and lemmatising all text.

Named-entity recognition

To identify the targets of hate speech, Named Entity Recognition (NER), a natural language processing (NLP) task that detects and identifies entities that

are present in a piece of text, was performed. An open-source library, spaCy (Honnibal & Montani, 2017), was used and fine-tuned to detect and identify the local targets of hate speech (e.g., trained to recognise local organisational bodies).

Topic classification

Bidirectional Encoder Representations from Transformers (BERT)³ – a state-of-the-art deep learning method for NLP tasks – was used to identify and classify text into 8 predefined levels of hate intensity. Using an adapted version of the hate-speech intensity scale developed by Bahador et al. (2019), we identified 8 levels of hate intensity based on the salient narratives of the local data (see Table 1).

SingBERT, a BERT-based model fine-tuned on colloquial Singlish and Manglish⁴ data (Lim, 2021), was further fine-tuned⁵ for the study's context. The accuracy of the BERT-based classifier (f1-score = 0.82) was comparable to results found in other similar text classification studies (Chalkidis et al., 2019; Nikolov & Radivchev, 2019; Yada et al., 2022). This fine-tuned model was then applied to the full dataset to predict the hate intensity level of each text message. Posts and comments were retained for analysis if the predicted label had >.50 probability of being selected by the model over other possible labels.

RESULTS AND DISCUSSION

Prevalence of hate speech

A time-series graph was plotted to identify the pattern of hate speech text over the time period of 12 March 2016 to 30 September 2021. Hate speech

² CECA is a free trade agreement signed in 2005 to increase trade and market access between Singapore and India (Enterprise Singapore, n.d.).

³ BERT is an open-source model developed by Google to understand the contextual embeddings of human words (Devlin et al., 2018). It is pre-trained on a large corpus of unlabelled text including the entire Wikipedia (~2,500 million words) and Book Corpus (~800 million words). BERT has achieved state-of-the-art performance on a wide range of NLP tasks and has been widely used by studies that analyse and interpret human language (Devlin et al., 2018; Rogers et al., 2020).

⁴ Singlish and Manglish refer to a mixture of English, Mandarin, Tamil, Malay, and other local dialects like Hokkien, Cantonese, Teochew. SingBERT was trained on data collected from subreddits -r/Singapore and r/Malaysia, and forums such as hardwarezone.

⁵ To train and fine-tune the SingBERT, 2416 posts and comments were extracted and manually categorised into the predefined levels of hate intensity to form the testing data. 14800 training data were created by randomly sampling records from each category, which was subsequently paraphrased in 10 multiple ways using the Pegasus transformer, a deep-learning model used for paraphrasing and summarising text data (Zhang et al., 2019). This was done to make the categorising process robust based on the content of the text rather than idiosyncratic writing styles. For the fine-tuning process, dropout probability was set at 0.2, number of epochs at 20, and initial learning rate at 5e-6.

Table 1. Predefined labels of hate intensity, as adapted from Bahador's et al. (2019) hate-speech intensity scale

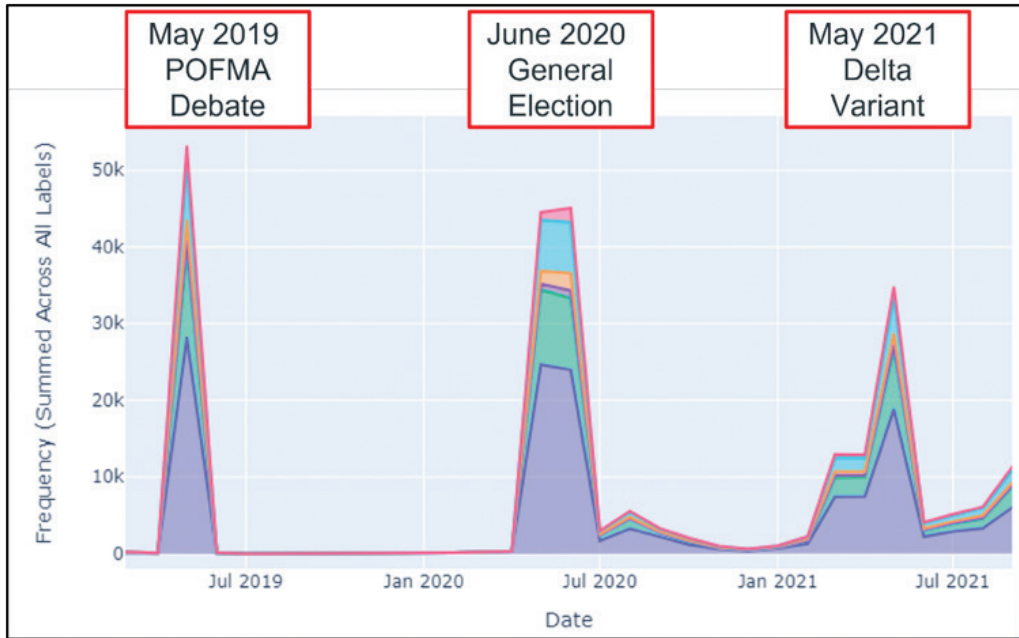
Label	Description	Examples
Non-hate (0)	Expressions that do not show a clear sign of hate (i.e., do not fall in the higher levels)	<i>So much facepalm</i>
Us vs them (1)	Expressions that differentiate between an in-group and out-group and highlight an us-vs-them attitude. Examples include negative generalisations and stereotypes about the out-group.	<i>Only they or FT [foreign talents] can sue. Ordinary citizens cannot.</i>
Threat (2)	Expressions that identify actual or perceived threats from out-groups, which include: <ol style="list-style-type: none"> Realistic threats: tangible threats to the well-being of the in-group; and Symbolic threats: intangible threats to the culture or identity of the in-group 	<i>They should not bring their culture to Singapore and look down upon Singaporeans</i>
Negative Actions (3)	Expressions that call for non-violent negative actions to be done to the out-group.	<i>Expressions of avoidance and exclusion; vote them out</i>
Negative Character (4)	Expressions that associate the out-group with negative traits or characteristics .	<i>Stupid; lazy; entitled; hypocrites; bastards; idiot</i>
Dehumanising & Demonising (5)	Expressions that associate the out-group with subhuman or superhuman characteristics .	<i>Evil one, parasite, pigs, self-entitled like gods, monsters</i>
Violence (6)	Expressions that call for actual or metaphorical non-lethal harm to the out-group, including wishes for out-group to be infected with disease/virus. Expressions of actual or metaphorical non-lethal harm by out-group towards in-group.	<i>I really hope he gets raped; punch her face; I hope he gets infected; they are molesters and kidnappers</i>
Death (7)	Expressions that call for actual or metaphorical lethal harm to the out-group.	<i>Go kill yourself; they are all murderers</i>

was found to drastically peak and drop on certain dates. Specifically, the peaks in Figure 3 correspond to the parliamentary debates about the Protection from Online Falsehoods and Manipulation Act (POFMA) in May 2019, the General Elections in June 2020, and the emergence of the Delta variant of COVID-19 in May 2021. This is aligned with past observations where hate speech tends to peak during times of uncertainty, or if certain threats are made more salient (Hackett, 2021). This is in line with the integrated threat theory, which states that

hate is heightened when others are perceived as realistic and symbolic threats (Stephan & Stephan, 2000). Realistic threats include threats of physical harm such as disease and competition for jobs, while symbolic threats arise from perceived differences between the values and worldview of the in-group and out-group, such as the dilution of a culture.

Such threats are made more salient during crises, prompting people to look for someone to blame in order to manage their fears and feelings of

Figure 3. Frequency of hate posts and comments between June 2019 and September 2021

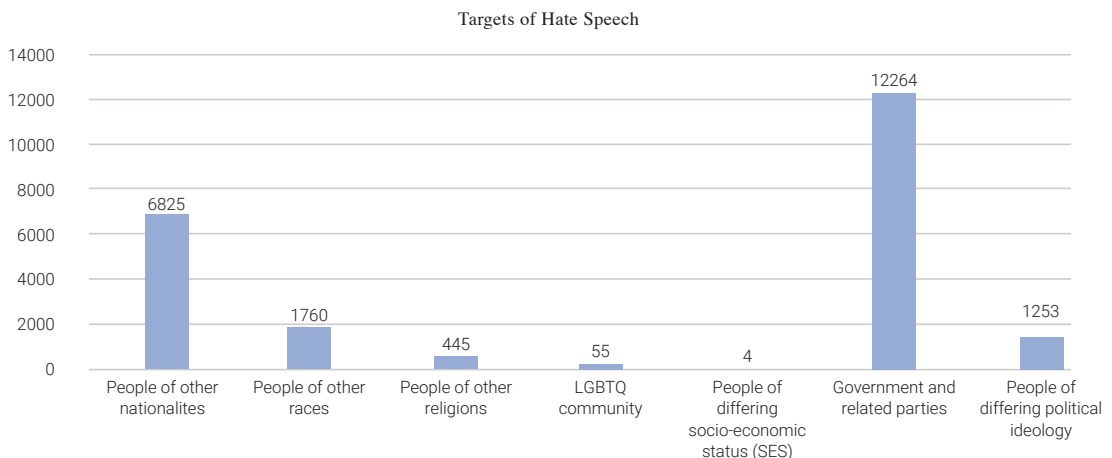


distress (Cichocka et al., 2015; Šrol et al., 2022), thus resulting in an influx of hate speech (Diers-Lawson, 2020). For instance, during the COVID-19 pandemic, anti-Asian hate speech in the United Kingdom and United States grew by 1662% in 2020 compared to 2019 (Hackett, 2021). Similarly, a European Union research initiative, Specialised Cyber-Activist Network (SCAN), found various salient narratives that scapegoated different communities. Some of these narratives adapted existing stereotypes and prejudices to the COVID-19 situation (SCAN, 2020).

Targeted out-groups

With the use of NER, 7 main targeted out-groups were identified based on the frequency of hate posts and comments from the period of 12 October 2016 to 30 September 2021: people of other nationalities, people of other races, people of other religions, the LGBTQ community, people of other socio-economic status (SES), people with differing political ideology, and people in or associated with the government (e.g., the ruling party, statutory boards, government agencies, law enforcement). Figure 4 shows the

Figure 4. Bar chart showing the number of Facebook posts and comments targeting each specific out-group



number of hate posts and comments that target the different out-groups. Unsurprisingly, the highest frequencies reflect the common topics of concern and social fault lines (e.g., race, nationality) in the local online discourse (Mathews et al., 2019).

Notably, the government was found to be the most targeted out-group, suggesting that online users in Singapore tend to attribute their grievances to the failure of the government. For example, with the emergence of the COVID-19 Delta variant in Singapore, related hate speech targeted not only foreigners, who were perceived to be virus carriers, but also the government, who were perceived to be gatekeepers and were expected to protect Singaporeans from the pandemic. This is seen in the following Facebook comment:

[Singapore] is just a country with corrupted government that loves money as well. You die, [it is] your business, and you better die so they can import more of their favourite CECA[,] COVID, fake degrees, and rapists are of no concern to them.

Facebook comment dated 2 August 2021

This was seen overseas as well, where the COVID-19 pandemic resulted in a surge of anti-government sentiments, especially in the early phases of the pandemic when the rapid spread of the virus resulted in widespread panic among netizens, and changing public health measures (e.g., mask mandates, vaccinations) were met with confusion and feelings of doubt (Tyson & Funk, 2022). In the US, the Pew Research Center observed declining ratings for public health and elected officials' responses to the COVID-19 outbreak, with 49% of survey respondents rating their government as doing a poor or fair job while the positive ratings were lower by 10% compared to findings in 2021 (Tyson & Funk, 2022). In some cases, extremists even used the pandemic to buttress anti-government, anti-immigrant, and racist rhetoric (Campion et al., 2021). For example, a common far-right conspiracy theory claimed that governments were using the pandemic to infringe on citizens' civil liberties (Marone, 2022).

Hate intensity

Figure 5 shows the percentage of posts and comments for each hate intensity level. Hate speech seems to be more prevalent at moderate levels of hate intensity (e.g., negative character and demonising and dehumanising). As mentioned

Figure 5. Pie chart showing the percentage of Facebook posts and comments according to hate intensity level

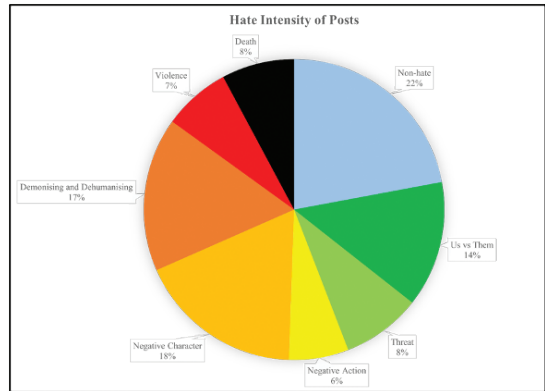
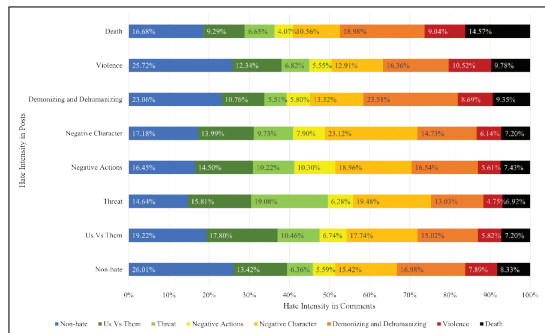


Figure 6. Bar chart detailing the hate intensity of comments to corresponding hate intensity level of post



earlier, not many studies have explored hate intensity of online hate speech in the same manner as this study. Although we cannot draw comparisons to many other studies, the lower proportions of high levels of hate speech (i.e., violence and death) here reflect an optimistic view of the sampled Singaporean social media behaviours. Due to the strict stance that the Singapore government has taken against online hate speech, it is possible that most netizens are not inclined to post violence and death content due to perceived moral violations or for concerns of violating applicable laws, such as the Protection from Online Falsehoods and Manipulation Act (POFMA), the Maintenance of Religious and Racial Harmony Act, and Protection from Harassment Act (POHA).

Figure 6 illustrates the distribution of speech based on the hate intensity of posts and comments. Regression analysis found that posts with higher

intensity levels tend to be significantly associated with comments of higher hate intensity levels, $\beta = .0428$, $SE = .002$, $p < .001$). This supports ‘homophily’ – the tendency for individuals’ personal networks to be more homogenous than heterogenous (Khanam, 2020; McPherson et al., 2001). It is possible that such posts attract the attention of others with the same beliefs, priming them to comment with their own agreement. These commenters fall prey to cognitive biases, such as confirmation bias, which is the tendency to engage with information that supports one’s existing beliefs (Mothes, 2017). In the online space, confirmation bias is prevalent during discourses of controversial issues; netizens appear to believe their derogatory perspectives and seek to reinforce their own and like-minded others’ beliefs (Thompson & Woodger, 2020). This can thus result in the reproduction of further hate speech in subsequent comments and even an escalation of hate speech intensity (Thompson & Woodger, 2020). For example, in one post that discussed the foreign workforce in Singapore, the poster insinuated that some of them had fake qualifications: “When FT = Fake Talent. What is MOM doing?” In response, some commenters echoed similar sentiments, with comments such as, “Not fake talent, correct term is foreign trash”. In this case, the hate intensity escalated up one level from negative character to demonising and dehumanising. While not a drastic jump in hate intensity level, for higher hate intensity posts, the hate intensity of their comments did tend to aggregate around similar intensity levels.

However, the above regression analysis also found the effect size to be extremely small ($R^2 = .001$). In other words, 0.1% of the variability observed in hate intensities of comments is explained by hate intensities of posts. This may be explained by past research which has found that high-hate comments arise not only from high-hate posts, but also high-hate comments (Dahiya et al., 2021). In a study examining the hate intensity of Twitter posts and replies, Dahiya and colleagues (2021) found no significant correlation between the hate levels of posts and replies, noting that the hate intensity of reply threads had highly diverse patterns. In fact, they noticed that the original post may not be hateful but the reply thread can be if there are hateful comments, which then provoke others to reply similarly. Indeed, our study observed similar patterns, where non-hate posts gave rise to comments of higher hate intensity levels.

IMPLICATIONS AND LIMITATIONS

Identifying intensities of hate speech

One of the main aims of this study is to identify the trends and prevalence of hate speech on local social media platforms, to foster awareness, accountability and de-escalation (Bahador et al., 2019). The study has revealed the prevalent social fault lines and topics that are causing growing concerns or unrest amongst the sampled Singaporean netizens. However, findings may not be generalisable to all netizens and all demographics in Singapore as data was collected from select Facebook pages.

Studies conducted in 2020 revealed that the majority of Facebook users in Singapore were aged between 25 and 44 years old, while 85% of Instagram users in Singapore were between the ages of 16 and 24 years old (Heng, 2022). While not entirely representative, there is value in exploring such vocal groups as they can provide insight into certain public anxieties. Past research has also found that hate speech travels farther, wider, and more virulently than non-hate content (Mathew et al., 2019). Although they may be a vocal minority, it is important for the government to be tuned in as there is always potential for such negative sentiments to fester and grow. If similar methods were to be applied on a larger scale, this can inform policy makers and other government agencies on the appropriate measures to take to alleviate public anxieties which, if left unaddressed, might not only affect their trust in the government but also transform into anti-government hate.

In the long term, as part of ground-sensing efforts, hate speech on online platforms can serve as a “thermometer” of the level of hate in the local context, where rising hate levels may indicate escalating sentiments of intolerance and act as early warning signs for violent and physical manifestations of hate (Bahador et al., 2019). Accordingly, such observations can also be useful in informing resource allocation in efforts to mitigate the impact of hate speech (Quinn, 2019). The hate intensity scale may be used by content moderators, practitioners, and other relevant government agencies as a guide to prioritise posts or comments of higher hate intensity for timely intervention and moderation. Policymakers can also direct more resources to intervention measures that are

enforced on higher levels of hate intensity to prevent escalation into physical acts of hate.

However, users of the hate intensity scale should be cautioned that the scale used in the current study serves as a mere exploratory classification of hate speech according to its apparent severity and intensity levels, and the dataset is not representative of hate speech in all contexts. Further research and validation need to be conducted before it can be used as a prescriptive checklist.

One research question worth exploring is the transmission of online hate speech into real-life hate behaviours, so as to identify the threshold of hate speech requiring intervention and mitigation measures. In addition, the current study primarily used an offender-centric perspective, which focused on the content and intent of the source in determining its hate intensity and target out-group. However, when determining intervention and management strategies, it is also important to consider the impacts of hate speech and from a victim-centric angle (e.g., inter-group tension, emotional reactions of members of the target out-group; Henson et al., 2013; Müller & Schwarz, 2020). Future research can attempt to refine the hate speech intensity scale such that it reflects the scale of impact of hate speech, and to include a more comprehensive guide on the appropriate response and intervention measures required for each level of hate speech.

Countering speech as a response

However, researchers and policymakers have increasingly recognised that removing harmful content alone is not sufficient in fighting online hate speech, as it has been criticised for merely moving hate from one platform to another, rather than eliminating it (Chandrasekharan et al., 2017). Considering that the hate in comments might have a larger impact on hate levels in other comments than that of the original post (Dahiya et al., 2021), counter speech is a potential alternative strategy to directly defuse hate speech.

Counter speech refers to direct responses (e.g., comments, replies, etc.) to hateful content that are aimed “to stop it, reduce its consequences, discourage it, as well as to support the victim and fellow counter speakers, and ultimately increase civility and deliberation quality of online

discussions” (Garland et al., 2022). Like hate speech, counter speech can take many forms, such as providing facts, pointing out logical inconsistencies in hateful messages, supporting victims, or even flooding the discussion with neutral or unrelated content (Hangartner et al., 2021). In a study that compared the effectiveness of diverse types of counter speech, Hangartner and colleagues (2021) found that the use of empathy in counter speech within the comments section was more consistently effective in defusing hateful discourse compared to the use of humour and warnings of consequences. This may suggest the vital role of empathy in reducing exclusionary and hostile sentiments towards target outgroups. Future studies may also explore the effectiveness of various counter speech strategies in the local context. Counter speech is a nascent but promising form of direct intervention that has been increasingly employed by numerous international and non-governmental organisations to defuse and reduce online hate speech (Hangartner et al., 2021). Policymakers can thus explore means of leveraging counter speech as an intervention for online hate speech and allocating resources to make it more scalable.

Countering using bystanders

In general, counter speech is still relatively understudied and much remains to be known with regards to its effectiveness in curbing the spread of hatred online. However, research on cyberbullying, a phenomenon that shares many similarities with hate speech in terms of causes and manifestations (Blaya & Audrin, 2019), has shed light on the effectiveness of organised efforts as compared to independent individual efforts in tackling hate speech (Garland et al., 2022). Specifically, bystanders often look to others when deciding whether to actively oppose the bullying or hate and help the victim. Thus, lone efforts in countering hate speech may often seem futile, as individuals who attempt to counter hateful messages by themselves in a flood of similar messages may easily become victims of online hate themselves (Buerger, 2020). Additionally, the presence of counter hate messages can serve as an indication of the social norm – a large volume of messages that oppose the hateful message may be perceived as a signal that hate is not tolerated in the overall population (Álvarez-Benjumea & Winter, 2018; Matias, 2019). These perceptions can then

guide people's reactions to and acceptance of hate and counter hate discourse, encouraging and mobilising more netizens to vocalise their counter speech expressions online (Garland et al., 2022). Accordingly, government agencies may want to work with community-based organisations that wish to engage in counter speech efforts; they would achieve increased effectiveness if they organised and participated in online discourse in a coordinated way (Garland et al., 2022; Buerger, 2020).

USE OF DEEP LEARNING TECHNIQUES

With the increase in global use of technology, there is a wealth of information available online for analysis. By applying data analytics and deep learning techniques, government agencies can analyse readily available data to gather ground sentiments in a much more efficient manner, as compared to conventional techniques (e.g., polls, manual analysis) that would otherwise prove to be a herculean effort. Eventually, this technology may be further developed to achieve automatic classification of real-time data to inform real-time decision making. While the technology for such applications is still nascent, policymakers can utilise more resources for such efforts to grow and explore their use for Singapore's security and social cohesion.

For example, as part of a pilot programme, the Institute for Strategic Dialogue in the United Kingdom developed a machine learning and NLP-based tool to

identify signs of radicalisation in social media activity (Davey et al., 2018). NLP capabilities were applied to examine comments on select public pages and flag instances of violent or aggressive language. The tool was also able to identify users demonstrating radical online behaviours such as posting radical content, liking radical posts, and being part of an online network with others whom law enforcement had identified as radical. The pilot programme was able to significantly narrow down potentially radical social media users for intervention from 42,000 individuals to 7,000. This number was then further reduced after a manual review. 800 individuals were later identified for intervention in existing counter-radicalisation programmes. Such pilot programmes demonstrate the potential and value that deep learning techniques have when integrated into existing interventions for dealing with security and social cohesion issues.

Although this study employed NLP techniques and models that have been fine-tuned based on local data, the researchers noticed that the models faced difficulties understanding and classifying the text, especially when it came to incorporating the contextual cues of language, such as sarcasm and metaphors. Thus, most modern hate speech monitoring techniques continue to involve a mixture of manual and automated processes (Quinn, 2019). The current study is also limited to text data, but future studies may wish to consider expanding the sources to include other expressions of hate, such as memes and videos.

ABOUT THE AUTHORS



Hong Jingmin

is a Psychologist with the Operations and Forensic Psychology Division of the Police Psychological Services Department, Singapore Police Force. She manages the Victim Care Cadre Programme and provides psychological support for police operations, crime investigations, and victim support. Previously, she was a psychologist with the Resilience, Safety and Security Psychology Branch of the Home Team Behavioural Sciences Centre⁶, where she researched and presented on areas such as violent extremism, hate crimes and hate speech.

⁶ The Home Team Behavioural Sciences Centre (HTBSC) has since undergone a reorganisation and is now referred to as the Home Team Psychology Division. The Division was formed in Ministry of Home Affairs, Singapore on 1 February 2023, from the merger of the HTBSC, the Office of Chief Psychologist, and the Centre for Advanced Psychological Sciences.



Nur Aisyah Abdul Rahman

was formerly a Senior Behavioural Sciences Research Analyst with the Home Team Behavioural Sciences Centre. Her key areas of research include social fault line concerns, such as prejudice and race and religious issues, as well as understanding violent extremism and hate from a psychological perspective. With the findings from her research, she developed and conducted training modules for Home Team officers. Some of her research has also been published and presented at local and international conferences.



Gabriel Ong

is a Senior Principal Psychologist and Deputy Director with the Community and Communications Psychology Branch of the Home Team Psychology Division. His primary role at the Division includes overseeing research on issues such as social and community resilience in order to support policy and operations on issues of national security. Concurrently Deputy Director of the Psychological and Correctional Rehabilitation Division of the Singapore Prison Service, he also oversees correctional research, programme design and evaluation, and operational psychology, in order to inform and ensure the formulation of evidence-based correctional policies and practices. A clinical psychologist by training, Gabriel is also an adjunct lecturer with the Nanyang Technological University, Singapore.



Shamala Gopalakrishnan

holds a master's in Clinical Forensic Psychology from King's College London. She is currently Assistant Director with the Community and Communications Psychology Branch at the Home Team Psychology Division. Using a psychological and behavioural sciences perspective, the branch looks into the understanding of trends and issues concerning areas such as psychology of hate and community resilience. Prior to joining the Division, Shamala worked as a prison psychologist for 8 years. There, she conducted risk assessments and interventions for both adult and youth offenders with violence and sexual violence offending behaviours.



Majeed Khader

is the Chief Psychologist of the Ministry of Home Affairs, and leads the Home Team Psychology Division. A trained crisis negotiator, he is also Associate Professor (Adjunct) at both the National University of Singapore and the Nanyang Technological University. He has published widely and is the author of *Crime and Behaviour*, and co-editor of several books, including *Introduction to Cyber Forensic Psychology*, *Prepared for Evolving Threats: The Role of the Behavioural Sciences*, and *Combatting Violent Extremism in the Digital Era*. He plays a key role in leading, directing, and guiding practice, research, training, and operational support of various behavioural sciences domains.

ACKNOWLEDGEMENTS

With inputs from:

Ken Chen, Senior Research Analyst, Home Team Psychology Division

Lin Yuan, Intern, formerly with Home Team Behavioural Sciences Centre

Hanan Huang, Intern, formerly with Home Team Behavioural Sciences Centre

Haziq Hassan, formerly Psychologist with the Home Team Behavioural Sciences Centre

REFERENCES

- Álvarez-Benjumea, A., & Winter, F. (2018). Normative change and culture of hate: An experiment in online environments. *European Sociological Review*, 34(3), 223-237.
- Anderson, L., & Barnes, M. (2022, January 25). *Hate speech*. *Stanford Encyclopedia of Philosophy*. <https://plato.stanford.edu/entries/hate-speech/#DogwCodeLang>
- ARTICLE19. (2015). 'Hate speech' explained: A toolkit. <https://www.article19.org/data/files/medialibrary/38231/'Hate-Speech'-Explained---A-Toolkit-%282015-Edition%29.pdf>
- Ayo, F. E., Folorunso, O., Ibharalu, F. T., & Osinuga, I. A. (2020). Machine learning techniques for hate speech classification of twitter data: State-of-the-art, future challenges and research directions. *Computer Science Review*, 38, 100311.
- Ayoub, J., Yang, X. J., & Zhou, F. (2021). Combat COVID-19 infodemic using explainable natural language processing models. *Information Processing & Management*, 58(4), 102569.
- Bahador, B., Kerchner, D., Bacon, L., & Means, A. (2019). *Monitoring hate speech in the US media*. Working Paper. <https://mediapeaceproject.smpa.gwu.edu/report-2/>
- Buerger, C. (2020). The anti-hate brigade: how a group of thousands responds collectively to online vitriol. *Available at SSRN*: <https://dx.doi.org/10.2139/ssrn.3748803>
- Blaya, C., & Audrin, C. (2019, June). Toward an understanding of the characteristics of secondary school cyberhate perpetrators. In *Frontiers in Education* (Vol. 4, p. 46). Frontiers Media SA. <https://doi.org/10.3389/educ.2019.00046>
- Broadcasting Complaints Commission of South Africa. (2017). *Hate speech*. <https://www.bccsa.co.za/faq-items/hate-speech/>
- Campion, K., Ferrill, J., & Milligan, K. (2021). Extremist Exploitation of the Context Created by COVID-19 and the Implications for Australian Security. *Perspectives on Terrorism*, 15(6), 23-40. <https://www.jstor.org/stable/27090914>
- Chalkidis, I., Androutsopoulos, I., & Aletras, N. (2019). Neural legal judgment prediction in English. *arXiv preprint arXiv:1906.02059*.
- Chandrasekharan, E., Pavalanathan, U., Srinivasan, A., Glynn, A., Eisenstein, J., & Gilbert, E. (2017). You can't stay here: The efficacy of reddit's 2015 ban examined through hate speech. *Proceedings of the ACM on Human-Computer Interaction*, 1(CSCW), 1-22.
- Chen, X. K., Na, J. C., Tan, L. K. W., Chong, M., & Choy, M. (2022). Exploring how online responses change in response to debunking messages about COVID-19 on WhatsApp. *Online Information Review*. <https://www.emerald.com/insight/content/doi/10.1108/OIR-08-2021-0422/full/html>
- Cichočka, A., de Zavala, A. G., Marchlewska, M., & Olechowski, M. (2015). Grandiose delusions: Collective narcissism, secure in-group identification, and belief in conspiracies. In *The psychology of conspiracy* (pp. 60-79). Routledge.
- Cinelli, M., De Francisci Morales, G., Galeazzi, A., Quattrociocchi, W., & Starnini, M. (2021). The echo chamber effect on social media. *Proceedings of the National Academy of Sciences*, 118(9), e2023301118. <https://doi.org/10.1073/pnas.2023301118>
- Council of Europe Committee of Ministers. (1997). Recommendation No. R 97(20) on of the Committee of Ministers to Member States on "Hate Speech". <https://rm.coe.int/1680505d5b>
- Corazza, M., Menini, S., Cabrio, E., Tonelli, S., & Villata, S. (2020). A multilingual evaluation for online hate speech detection. *ACM Transactions on Internet Technology (TOIT)*, 20(2), 1-22. https://dl.acm.org/doi/abs/10.1145/3377323?casa_token=qC07Grzx8HAAAAAA%3A-9t2CrLLQzY6l-7gaaAQYkl6GeYHKghJXFoceelqyej1otmfnlMsmekvXow-c6EQqalJzRS0fJHj

- Dahiya, S., Sharma, S., Sahnan, D., Goel, V., Chouzenoux, E., Elvira, V., ... & Chakraborty, T. (2021, August). Would your tweet invoke hate on the fly? forecasting hate intensity of reply threads on twitter. In *Proceedings of the 27th ACM SIGKDD Conference on Knowledge Discovery & Data Mining* (pp. 2732-2742).
- Davey, J., Birdwell, J., & Skellett, R. (2018). *Counter conversations: A model for direct engagement with individuals showing signs of radicalisation online*. Institute for Strategic Dialogue. <https://www.isdglobal.org/isd-publications/counter-conversations-a-model-for-direct-engagement-with-individuals-showing-signs-of-radicalisation-online/>
- Devlin, J., Chang, M. W., Lee, K., & Toutanova, K. (2018). Bert: Pre-training of deep bidirectional transformers for language understanding. *arXiv preprint* <https://doi.org/10.48550/arXiv.1810.04805>
- Diers-Lawson, A. (2020). Applying the stakeholder relationship model as an issue management and risk communication tool. <https://doi.org/10.3726/b17931>
- Enterprise Singapore. (n.d.). *India-Singapore Comprehensive Economic Cooperation Agreement (CECA)*. Retrieved July 20, 2021, from <https://www.enterprisesg.gov.sg/non-financial-assistance/for-singapore-companies/free-trade-agreements/ftas/singapore-ftas/ceca>
- Garland, J., Ghazi-Zahedi, K., Young, J. G., Hébert-Dufresne, L., & Galesic, M. (2022). Impact and dynamics of hate and counter speech online. *EPJ data science*, 11(1), 3. <https://epjdatascience.springeropen.com/track/pdf/10.1140/epjds/s13688-021-00314-6.pdf>
- Hackett, L. (2021). *Uncovered: Online hate speech in the covid era*. Ditch the Label. <https://www.ditchthelabel.org/research-papers/hate-speech-report-2021/>
- Hangartner, D., Gennaro, G., Alasiri, S., Bahrnich, N., Bornhoft, A., Boucher, J., ... & Donnay, K. (2021). Empathy-based counterspeech can reduce racist hate speech in a social media field experiment. *Proceedings of the National Academy of Sciences*, 118(50), e2116310118.
- Hatewatch. (2021). Who are the Boogaloos, who were visible at the Capitol and later rallies? Southern Poverty Law Center. <https://www.splcenter.org/hatewatch/2021/01/27/who-are-boogaloos-who-were-visible-capitol-and-later-rallies>
- Heng, W. L. M. (2022, January 3). The Complete Guide to Social Media Statistics in Singapore. *BestinSingapore*. Retrieved September 28, 2022, from <https://www.bestinsingapore.co/singapore-social-media-statistics/>
- Henson, B., Reyns, B. W., & Fisher, B. S. (2013). Fear of crime online? Examining the effect of risk, previous victimization, and exposure on fear of online interpersonal victimization. *Journal of Contemporary Criminal Justice*, 29(4), 475-497. <http://dx.doi.org/10.1177/1043986213507403>
- Honnibal, M., & Montani, I. (2017). spaCy 2: *Natural language understanding with Bloom embeddings, convolutional neural networks and incremental parsing*.
- Khanam, K. Z., Srivastava, G., & Mago, V. (2020). The homophily principle in social network analysis. *arXiv preprint arXiv:2008.10383*.
- Lim, Z. [@zanelim]. (2021, May 20). *SingBERT*. <https://huggingface.co/zanelim/singbert>
- Marone, F. (2022). Hate in the time of coronavirus: exploring the impact of the COVID-19 pandemic on violent extremism and terrorism in the West. *Security Journal*, 35(1), 205-225.
- Marshall, A. R. (2013, June 27). Myanmar gives official blessing to anti-Muslim monks. *Reuters*. <https://www.reuters.com/article/us-myanmar-969-specialreport-idUSBRE95Q04720130627>
- Mathew, B., Dutt, R., Goyal, P., & Mukherjee, A. (2019, June). Spread of hate speech on online social media. In *Proceedings of the 10th ACM conference on web science* (pp. 173-182). <https://arxiv.org/pdf/1812.01693>
- Mathews, M., Tay, M., & Selvarajan, S. (2019). *Faultlines in Singapore: Public Opinion on Their Realities, Management & Consequences* (No. 37). IPS Working Papers. https://lkyspp.nus.edu.sg/docs/default-source/ips/working-paper-37_faultlines-in-singapore_public-opinion-on-their-realities-management-and-consequences_final.pdf

- Matias, J. N. (2019). Preventing harassment and increasing group participation through social norms in 2,190 online science discussions. *Proceedings of the National Academy of Sciences*, 116(20), 9785-9789.
- McPherson, M., Smith-Lovin, L., & Cook, J. M. (2001). Birds of a feather: Homophily in social networks. *Annual review of sociology*, 415-444. <https://doi.org/10.1146/annurev.soc.27.1.415>
- Mothes, C. (2017). Confirmation bias. In F. Moghaddam (Ed.), *The SAGE encyclopedia of political behavior* (pp. 125-125). SAGE Publications, Inc., <https://dx.doi.org/10.4135/9781483391144.n61>
- Mozur, P. (2018, October 15). A Genocide Incited on Facebook, With Posts From Myanmar's Military. *The New York Times*. <https://www.nytimes.com/2018/10/15/technology/myanmar-facebook-genocide.html>
- Müller, K., & Schwarz, C. (2020). Fanning the flames of hate: Social media and hate crime. *J. Eur. Econ. Assoc.* 19, 2131–2167.
- Nikolov, A., & Radivchev, V. (2019, June). Nikolov-radivchev at semeval-2019 task 6: Offensive tweet classification with bert and ensembles. In *Proceedings of the 13th international workshop on semantic evaluation* (pp. 691-695).
- Quinn, T. (2019). Monitoring hate speech: Challenges and Strategies. *Hatebase*. https://www.ohchr.org/sites/default/files/Documents/Issues/Racism/IEE/Session6/TimothyQuinn_8May2019.pdf
- Rogers, A., Kovaleva, O., & Rumshisky, A. (2020). A primer in bertology: What we know about how bert works. *Transactions of the Association for Computational Linguistics*, 8, 842-866. <https://arxiv.org/abs/2002.12327>
- Shanmugam, K. (2019, April 1). *Ministerial Statement on Restricting Hate Speech to Maintain Racial and Religious Harmony in Singapore, Speech by Mr K Shanmugam, Minister for Home Affairs and Minister for Law*. Minister of Home Affairs. <https://www.mha.gov.sg/mediaroom/parliamentary/ministerial-statement-on-restricting-hate-speech-to-maintain-racial-and-religious-harmony-in-singapore-speech-by-mr-k-shanmugam-minister-for-home-affairs-and-minister-for-law/>
- Sedition (Repeal) Bill 2021 (23).
- Siegel, A. A. (2020). Online hate speech. *Social media and democracy: The state of the field, prospects for reform*, 56-88.
- Singh, M., Jakhar, A. K., & Pandey, S. (2021). Sentiment analysis on the impact of coronavirus in social life using the BERT model. *Social Network Analysis and Mining*, 11(1), 1-11.
- Smith, S. A. (2021, March 18). *Japan has weathered COVID-19 better than many, but problems persist*. Council on Foreign Relations. <https://www.cfr.org/in-brief/japan-covid-19-pandemic-response-restrictions-two-years>
- Specialised Cyber-Activist Network. (2020). *Hate speech trends during the Covid-19 pandemic in a digital and globalised age*. SCAN Project. <http://scan-project.eu/wp-content/uploads/sCAN-Analytical-Paper-Hate-speech-trends-during-the-Covid-19-pandemic-in-a-digital-and-globalised-age.pdf>
- Šrol, J., Cavojova, V., & Mikušková, E. B. (2022). Finding someone to blame: The link between COVID-19 conspiracy beliefs, prejudice, support for violence, and other negative social outcomes. *Frontiers in Psychology*, 12. <https://doi.org/10.3389/fpsyg.2021.726076>
- Statista. (2022). Social network penetration in Q3 2021. *Statista*. <https://www.statista.com/statistics/284466/singapore-social-network-penetration/>
- Stecklow, S. (2018, August 15). Why Facebook is losing the war on hate speech in Myanmar. *Reuters*. <https://www.reuters.com/investigates/special-report/myanmar-facebook-hate/>
- Stephan, W. S., & Stephan, C. W. (2010). An integrated threat theory of prejudice. In *Reducing prejudice and discrimination* (pp. 33-56). Psychology Press.
- Thompson, N., & Woodger, D. (2020). "I hope the river floods": online hate speech towards Gypsy, Roma and Traveller communities. *British Journal of Community Justice*, 16(1), 41-63.

Tyson, A. & Funk, C. (2022). *Increasing Public Criticism, Confusion Over COVID-19 Response in U.S.* Pew Research Center. <https://www.pewresearch.org/science/2022/02/09/increasing-public-criticism-confusion-over-covid-19-response-in-u-s/>

United Nations (n.d.). *Say #NoToHate -The impacts of hate speech and actions you can take*. Retrieved August 23, 2022, from <https://www.un.org/en/hate-speech>

Watanabe, H., Bouazizi, M., & Ohtsuki, T. (2018). Hate speech on twitter: A pragmatic approach to collect hateful and offensive expressions and perform hate speech detection. *IEEE access*, 6, 13825-13835. <https://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=8292838>

Yada, S., Nakamura, Y., Wakamiya, S., & Aramaki, E. (2022). Real-mednlp: Overview of real document-based medical natural language processing task. In *Proceedings of the 16th NTCIR Conference on Evaluation of Information Access Technologies*.

Yamamoto, A., & Jett, J. (2021, September 3). Japan's prime minister Suga to step down after year in office marked by Covid, Olympics. *NBC News*. <https://www.nbcnews.com/news/world/japan-s-prime-minister-suga-step-down-after-covid-olympics-n1278444>

Yin, W., & Zubiaga, A. (2021). Towards generalisable hate speech detection: a review on obstacles and solutions. *PeerJ Computer Science*, 7, e598. <https://www.ncbi.nlm.nih.gov/pmc/articles/PMC8237316/>

Zhang, J., Zhao, Y., Saleh, M., & Liu, P. (2020, November). Pegasus: Pre-training with extracted gap-sentences for abstractive summarization. In *International Conference on Machine Learning* (pp. 11328-11339). PMLR.

DIVERSE CULTURES, DIFFERENT LIARS

INSIGHTS INTO DECEPTION DETECTION IN CROSS-CULTURAL INTERACTIONS

Stephanie Chan & Stephenie Wong
Home Team Psychology Division, Ministry of Home Affairs, Singapore

ABSTRACT

The skill of making accurate lie-truth judgements is complex due to cross-cultural differences. As Singapore has reopened its borders to global travellers, the cultural diversity of people encountered by law enforcement officers is once again increasing substantially. Human lie detectors must flexibly consider the subtle differences in behaviours (i.e., kinesics, paralinguistics, and speech). This is essential as the lens of one's social and cultural expectations are subconsciously used to interpret observations and make split-second judgements of those we interact with. This brief reviews insights on cross-cultural communication which impact on deception detection, namely, the cultural variations in motivation, and the differences in certain body language and speech across cultures. The insights serve as knowledge to build our understanding of the cultural nuances in investigative contexts.

LAW ENFORCEMENT IN A MULTICULTURAL AND MULTI-ETHNIC COUNTRY

Singapore is a nation that is home and host to a diverse range of ethnicities and cultures. According to the Department of Statistics Singapore (SingStat), the total resident population of 4.07 million¹ includes 133,773 Singapore citizens and permanent residents who identify as "other ethnic groups" beyond the common categories of CMI – Chinese, Malay, and Indian (including Ceylonese) (SingStat, 2022). There are also some 170,000 employment pass holders (as at December 2022), mainly from India, China, Japan, Malaysia, the Philippines, and the United Kingdom, as well as 7,000 multinational companies located here as of 2021 (Wan, 2021). With the reopening of borders in 2022, 4 million to 6 million international visitors are projected by year end (Singapore Tourism Board, 2022). First

quarter statistics of visitor arrivals in Singapore have listed Indonesia, India, Malaysia, Australia, and the Philippines as the top five countries of origin, accounting for 56% of total international visitor arrivals (Singapore Tourism Board, 2022).

As a multicultural and multi-ethnic country, understanding the ways in which individuals from different cultures communicate is particularly useful for law enforcement officers who have to be able to distinguish between liars and truth-tellers, i.e. lie-truth detection, in investigative interviewing and border security contexts.

Culture influences the way people communicate verbally and through their nonverbal communications, including via facial expressions, voice tone, or gestures (Gregersen, 2005). People subconsciously rely on their culturally accepted ways of doing things, ways of interpreting

¹ According to SingStat (2022), the total population of Singapore as at end-June 2022 was 5.64 million, whereas the total resident population was 4.07 million. Singapore residents comprise citizens and permanent residents.

information, and preferences for interpersonal interactions. This brief focuses on cultural differences in three aspects of communication which may prove useful for investigative interviewing and deception detection contexts. Such contexts include face-to-face interactions, structured interviews, video and audio recordings, and the involvement of both witnesses and suspects. Cross-cultural communication via text or AI-mediated means will not be addressed here.

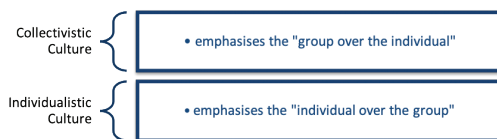
Data for this brief was gathered from sources such as print media, and articles from professional journals on communications, investigative interviewing, and deception detection. The aim is to highlight communication differences that are scientifically supported, to affirm and enhance current questioning and deception detection techniques being used by Home Team investigators.

DEFINING CULTURE

In the context of investigative interviewing, culture is defined as a dynamic and complex set of shared systems, meanings, and practices within a social group (Hope et al., 2022). Culture emerges from the histories and experiences of the group and is shaped by social interactions and relationships between the individual and wider society. In interactions and communications, it is expressed through, but not limited to, the individual's body language, facial expressions, speech (verbal) and nonverbal speech patterns.

The most common types of culture are Collectivistic Culture and Individualistic Culture (Gudykunst et al., 1996; Kim et al., 1998; Nishimura et al., 2008).

Figure 1. Quick comparison of collectivistic culture versus individualistic culture.



In a sense, the communication style of **Collectivistic Cultures** relies heavily on

- context to imply meaning and relay messages,
- non-verbal cues as added medium of

- communication, and
- relationships and social hierarchy to guide the direction of the interaction.

As viewed by an outsider, collectivistic cultures seem to communicate indirectly and require the listener to 'read between the lines' more often.

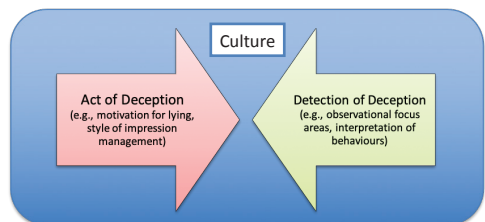
In contrast, the communication style of **Individualistic Cultures** relies heavily on the spoken or written message content. With less emphasis placed on the influence of societal relationships and hierarchies in interactions, individualistic culture favours direct communication. As viewed by an outside, individualistic cultures seem to pay greater attention to verbal communication and more obvious body language.

A caveat: Culture is experienced and interpreted differently based on the encounters and perspectives of everyone. We acknowledge that **in reality, countries do not fall neatly under an 'individualistic' or a 'collectivist' culture.** It is for the purpose of providing general knowledge and easy understanding that the differences between individualistic cultures and collectivistic cultures are highlighted in this brief.

How Does Culture Apply to Deception?

Culture influences deception in two ways (see Figure 2). Firstly, culture impacts the act of carrying out deception (Cheng & Broadhurst, 2005). Secondly, culture influences the decision-making processes of deception detection.

Figure 2. Influence of culture on both the act and the detection of deception.



The reason(s) interviewees lie may vary depending on their goal. For instance, an accomplice or a witness may be willing to cooperate in an interview but choose to lie about certain details to enhance their social image (i.e., 'saving face') and to protect

their own reputation (Lalwani et al., 2006; Lewis & George, 2008). In other instances, there are those who are motivated to lie to protect the honour of those whom they have social obligations towards (Burgoon et al., 2021). This tendency to protect group honour and maintain group dynamics is found more in collectivistic cultures.

Culture also influences the human lie detectors' decision-making processes. Cultural differences in communication could mean that officers' interpretations of another person's body language and speech could be vastly different from the interviewee's intended communication of information. For instance, a victim's lack of emotional expressiveness when describing a taboo situation (e.g., alleged marital rape) could cause that specific portion of the statement to be misconstrued as inauthentic.

To help craft behavioural 'baselines' of collectivistic cultures and individualistic cultures, we next explore the influence of culture on body language and speech cues.

INTERPRETING BEHAVIOURAL OBSERVATIONS USING THE LENS OF CULTURE

Observation #1: Kinesics (The Example of Emotional Expressiveness)

According to Ray Birdwhistell (1983, as cited in Waiflein, 2013) kinesics is the study of body language as part of communication. For example, someone who is excited may smile widely, make rapid hand gestures, and 'bounce' when they speak – an indication of high emotional expressiveness. The extent of emotional expressiveness can be useful in certain deception detection settings, e.g., a genuine traveller being asked about travel itinerary might display positive emotions of anticipation and eagerness (Warren et al., 2009; Zloteanu et al., 2021). However, human lie detectors must be informed that emotional displays vary by culture (Gudykunst & Ting-Toomey, 1998). Officers carrying out interpretations of emotional expressiveness by interviewees must do so with the knowledge of these 'baselines':



- Truth-tellers from Collectivistic Cultures have a social tendency to control and 'hold back' their (mostly negative) emotions in the presence of others, a trait that is valued in their cultures (Murata, Moser, & Kitayama, 2013). There is also a tendency to adjust emotional intensity to match that of the group or officer who they are speaking to (Eng, 2012).
- Truth-tellers from Individualistic Cultures valuing emotional expression tend to use movements and gestures to openly express their emotional state (Tsai et al., 2006).

Observation #2: Paralanguage (The Example of Pauses)

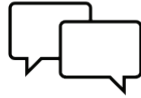
Paralanguage is the "vocal but nonverbal elements of communication by speech" (Key, 1975). This refers to nonverbal features such as volume, pitch, tone, hesitations, speaking rate (Qiang, 2013), and even consciously made laughs, sighs, coughs, etc. Many of these features have been used to differentiate liars from truth tellers in investigative interviews, with much empirical research support for pauses (i.e., variations include hesitation duration and response latency). A study by Stromwall and colleagues (2004) found that long pauses are used commonly by liars experiencing cognitive load, which is mental effort brought about by maintaining lies and concealing information. Once again, human lie detectors must be informed that pauses vary by culture. Officers carrying out interpretations of pauses by interviewees must do so with the knowledge of these 'baselines':



- Both truth-telling and lying individuals from Collectivistic Cultures tend to use greater frequencies of pauses and silences intentionally to convey nuanced meaning within social interactions during their conversations (Chung, 2013).
- Both truth-telling and lying individuals from Individualistic Cultures tend to use greater duration within pauses during conversations of a transactional nature (Ulijin & St Amant, 2000).

Observation #3: Verbal Speech (The Example of Details)

Speech is very useful for lie detection, even more compared to solely visual observations. Consistently, research has found that individuals shown video-only interviews have had the lowest accuracies in detecting deception (Davis, Markus, and Walters, 2006) compared to audio-only and audio-plus-video types of interviews (Bond & DePaulo, 2006). According to another study, Bond and Rao (2004) likewise found that when presented with speakers from a different culture, the deception detection accuracy rates were the highest when human lie detectors were given both audio and visual cues. In other words, the availability of speech cues for observation allows for more accurate lie and truth detection.



The volume of details, or pieces of information, given voluntarily by an interviewee can be very useful in distinguishing lies from truth. In particular, the number of verifiable details (i.e., details that can be checked or can be supported by collaborative evidence) provided by truth-tellers tends to be greater than that provided by liars, regardless of cultural influence (Leal et al., 2018; Taylor et al., 2014).

Example of a sentence with verifiable details:

I was looking through the menu at around 8pm at McDonalds and ordered a 10-piece McNuggets meal and Milo.

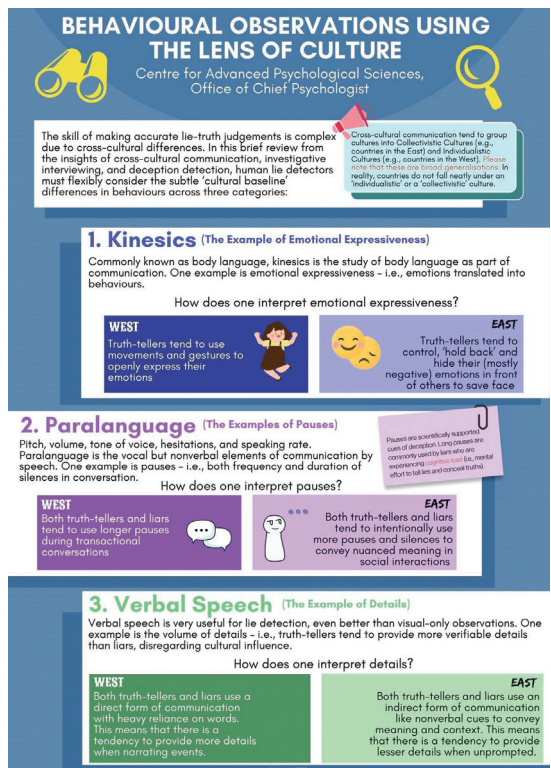
Within this sentence are details provided that allow for follow-up temporal and locational questioning and have the potential to be subsequently verified by CCTV footage, receipts, and the eyewitness testimonies.

However, human lie detectors must still take into account the influence of culture on verbal speech. Officers carrying out interpretations of the volume of verifiable details provided by interviewees must do so with the knowledge of these 'baselines':

- Both truth-telling and lying individuals from Collectivistic Cultures are used to an indirect form of communication involving nonverbal cues to convey meaning and context (Hall, 1976). There is thus a tendency for lesser details to be provided when unprompted during questioning.
- Both truth-telling and lying individuals from Individualistic Cultures are used to a direct form of communication with heavy reliance on words (Hall, 1976). Thus, there is a tendency for cooperative interviewees to provide more details within their narration of events.

In sum, these observational examples indicate the nuances brought about by culture. They remind us that interactions are complex exchanges of spoken and unspoken communication. Figure 3 summarises all three behavioural observational examples. The next section discusses broad strategies to be applied in investigative interviewing and questioning.

Figure 3. Infographic summarising some behavioural observations using the lens of culture



IMPROVING DETECTION OF DECEPTION ACROSS CULTURES: TWO BROAD STRATEGIES FOR LAW ENFORCEMENT OFFICERS

The three disciplines of culture communication, investigative interviewing, and deception detection are best positioned to provide insights to law enforcement and the broader criminal justice system. Research in this emerging area of cross-disciplinary work has outlined best practices for officers involved in interpreting truth and lie cues.

Improve Pattern Detection Capabilities

Everyone has expectations of how people behave, interact, and even lie (Castillo & Mallard, 2012). Such 'patterns' of behaviours assist us in our decision-making processes to enable decisions to be made under time-critical and information-scarce conditions. However, the Expectancy Violation Model states that we are sensitive to observed behaviours that are different from our expectations (i.e., outliers of our expected 'patterns'), to the extent that in the context of lie detection, these behaviours seem suspicious or deceitful (Bond et al., 1992; Levine et al., 2000). In other words, human lie detectors may unwittingly assume a truth-teller is a liar, or to a lesser extent, place the truth-teller under further scrutiny, if the behavioural and speech cues do not meet expectations.

For human lie detectors, it is important to expand our 'pattern' detection to make distinctions within cultures and across cultures (i.e., identify both culture baselines and general baselines). By recognising common cultural influences in the ways individuals behave and interact socially, better informed lie detection decisions can be made.

Tip 1: **Self-Awareness:**

Officers should map out their own parameters of what consists of expected behavioural observations – i.e., behavioural and speech patterns made by victims, witnesses, accomplices, perpetrators, crime types, demographics, etc. This allows officers to understand their existing 'patterns' and check their own assumptions.

Tip 2: **Seek Feedback:**

Officers should strive to obtain informative outcomes of their decisions – i.e., compare against corroborative evidence, generate several hypotheses to explain interviewee's behaviours, be alert to contradictory findings. This allows officers to counteract any instinctive judgements made on biases or stereotypes. Other methods to consider include holding feedback-consultative sessions with fellow colleagues and reviewing interview notes and past decisions.

By engaging in consistent self-awareness and feedback seeking processes, together with an attitude that 'there is always something new to learn', the constant exposure to various culture-influenced behaviours can improve and sharpen pattern detection over time, leading to improve lie and truth detection accuracies.

Aim for Culture-Based Cooperation Approaches

Culture-based cooperation approaches are developed more in organisational and business negotiations literature and are scarce within the investigative interviewing research domain. Nevertheless, investigative interviewing can benefit from a deeper understanding of culture-influenced motivations and goals and use the knowledge to increase interviewee's cooperation and lessen interviewee's uncertainty.

Tip 1: **Respect Face:**

Officers interviewing individuals from collectivistic cultures should avoid making statements that directly challenge the interviewee's loyalties or relationships with the group/community that they identify with. Officers interviewing individuals from individualistic cultures should avoid making statements that directly challenge the interviewee's self-image. This can be avoided by understanding the profile of the interviewee (i.e., identify interviewee's key relationship dynamics and micro-communities) during pre-interview preparation.

Tip 2: **Rephrase Sentences:**

Officers should make tactical adjustments to sentences to align with the interviewee's cultural values, motivations, and goals. For example, a sentence introducing the role of the interviewee

in the interview can be phrased as “What you share will help us to understand the situation” for individuals from collectivistic cultures; versus “What you share will help us to understand your actions” for individuals from individualistic cultures. This can be done through pre-interview identification of key sentences usually used to instruct or provide information on the interview process to the interviewee.

FUTURE DIRECTIONS AND RECOMMENDATIONS FOR THE HOME TEAM

Acknowledge the Value of Culture-Based Interviewing Approaches

The effort of obtaining accurate information requires a set of skills. For investigators who must interact with a diverse multicultural public, the various investigative skills (i.e., profiling, questioning, interviewing, and deception detection) can benefit from culture-based approaches that aim to increase cooperation during the interactions and thereby amplify the differences between truths and lies. Such knowledge can even be transferable to frontline officers who have more frequent interactions with members of the public. Given the potential for broad applicability of such skills, the Home Team should consider training programmes that include the domains of cultural communication for officers to hone their contributions in operations. The Home Team should also invest in in-house research on cultural communication that can be applied to operations in the local investigative interviewing context.

Tap on Cross-Discipline Knowledge

Culture communications usage in investigative interviewing and deception detection is still in its infancy in this region, and possibly internationally. However, much can be gathered and applied (wherever feasible) from the longstanding research disciplines of business negotiations, body motion communication, and cultural anthropology. It is hoped that this brief will encourage interest in the research findings and expertise from other disciplines for knowledge transfer to Home Team operations. The Home Team should build in-house expertise by being aware of the best practices and latest research developments in the aforementioned areas. Knowledge can be gleaned through seeking out thought leaders and then identifying concepts and frameworks that can be tailored to operational needs.

CONCLUSION

Distinguishing truths from lies across cultures is not an easy task because people bring along with them culturally accepted ways of sharing information, interpreting information, and interacting with others. Without knowledge of cultural differences in communication, decision-making for deception detection can unwittingly be hampered by individual biases and stereotypes, interviewee resistance, and overall miscommunication. As officers interact with residents and travellers from various cultures, it is important to understand cross-cultural communication in lying and truth-telling when forming judgements about a person’s truthfulness.

ABOUT THE AUTHORS



Stephanie Chan

is a Lead Psychologist with the Home Team Psychology Division. Stephanie’s current research interest is in crime and forensic psychology, particularly in the law enforcement context. Her primary research area focuses on the psychology of detecting deception and deceptive intent, as this has operational applications for cyber detection and people profiling purposes.



Stephenie Wong

is a former Behavioural Analyst at the Centre for Advanced Psychological Sciences (CAPS), which has been incorporated into the newly formed Home Team Psychology Division at the Ministry of Home Affairs. Her key areas of research included understanding cross-cultural communication and the detection of deception from a behavioural sciences and psychological perspective. In her time with CAPS, she also assisted in training officers on rapport building. At present, she remains in close contact with the psychologists and is looking to broaden her research interests.

The new Home Team Psychology Division (HTPD) was formed in the Ministry of Home Affairs on 1 February 2023, from the merger of the Home Team Behavioural Sciences Centre, the Office of Chief Psychologist, and the Centre for Advanced Psychological Sciences. HTPD comprises two directorates:

- Psychology Services Directorate, specialising in psychological assessment services
- Psychology Research Directorate, focusing on psychological research

The areas for services and research include leadership and talent psychology, mental resilience, criminal psychology, and community trauma in a crisis.

ACKNOWLEDGEMENTS

The authors would like to thank Chief Psychologist Dr Majeed Khader and Director Diong Siew Maan of the Home Team Psychology Division for their guidance and support, and intern Toh Jia Pei for her contribution of the infographic.

REFERENCES

- Bond, C. F., & DePaulo, B. M. (2006). Accuracy of deception judgments. *Personality and Social Psychology Review*, 10(3), 214-234.
- Bond, C. F., & Rao, S. R. (2004). Lies travel: Mendacity in the mobile world. In P. A. Granhag, & L. A. Stromwall (Eds.), *The Detection of Deception in Forensic Contexts* (pp. 127-147). Cambridge: Cambridge University Press.
- Burgoon, J. K., Metaxas, D., Nuamaker, J. F., & Ge, S. T. (2021). Cultural influence on deceptive communication. In *Detecting Trust and Deception in Group Interaction* (pp. 197-222). Springer, Cham.
- Castillo, P. A., & Mallard, D. (2012). Preventing cross-cultural bias in deception judgments: The role of expectancies about nonverbal behavior. *Journal of Cross-Cultural Psychology*, 43(6), 967-978.
- Chung, L. C. (2013). High-context cultures. *The Encyclopaedia of Cross-Cultural Psychology*, 2, 657-658.
- Chung, K. H., W., & Broadhurst, R. (2005). The detection of deception: The effects of first and second language on lie detection ability. *Psychiatry, Psychology and Law*, 12(1), 107-118. Doi: 10.1375/pplt.2005.12.1.107
- Davis, M., Markus, K. A., & Walters, S. B. (2006). Judging the credibility of criminal suspect statements: Does mode of presentation matter? *Journal of Nonverbal Behavior*, 30(4), 181-198.
- Eng, J. S. (2012). *Emotion and regulation and culture: The effects of cultural models of self on Western and East Asian differences in suppression and reappraisal*. University of California, Berkeley.

- Gregersen, T. S. (2005). Nonverbal cues: Clues to the detection of foreign language anxiety. *Foreign Language Annuals*, 38(3), 388-400.
- Gudykunst, W. B., Matsumoto, Y., Ting-Toomey, S., Nishida, T., Kim, K., & Heyman, S. (1996). The influence of cultural individualism-collectivism, self construals, and individual values on communication styles across cultures. *Human Communication Research*, 22(4), 510-543.
- Gudykunst, W. B., & Ting-Toomey, S. (1988). Culture and affective communication. *American Behavioral Scientist*, 31(3), 384-400.
- Hall, E. T. (1976). *Beyond culture*. New York: Anchor Press/ Double Day.
- Hope, L., Anakwah, N., Antfolk, J., Brubacher, S., P., Flowe, H., Gabbert, F., ... & Anonymous (2022). Urgent issues and prospects at the intersection of culture, memory, and witness interviews: Exploring the challenges for research and practice. *Legal and Criminological Psychology*, 27(1), 1-31.
- Key, M. R. (1975). *Paralanguage and Kinesics (Nonverbal Communication)*. New Jersey: Scarecrow Press.
- Kim, D., Pan, Y., & Park, H. S. (1998). High-versus-low-context culture: A comparison of Chinese, Korean, and American cultures. *Psychology & Marketing*, 15(6), 507-521.
- Lalwani, A. K., Shavitt, S., & Johnson, T. (2006). What is the relation between cultural orientation and socially desirable responding? *Journal of Personality and Social Psychology*, 90(1), 165.
- Leal, S., Vrij, A., Vernham, Z., Dalton, G., Jupe, L., Harvey, A., & Nahari, G. (2018). Cross-cultural verbal deception. *Legal and Criminological Psychology*, 23(2), 192-213.
- Lewis, C. C., & George, J. F. (2008). Cross-cultural deception in social networking sites and face-to-face communication. *Computers in Human Behavior*, 24(6), 2945-2964
- Murata, A., Moser, J. S., & Kitayama, S. (2013). Culture shapes electrocortical responses during emotion suppression. *Social Cognitive and Affective Neuroscience*, 8(5), 595-601. Doi: 10.1093/scan/nss36
- Nishimura, S., Nevgi, A., & Tella, S. (2008). Communication style and cultural features in high/low context communication cultures: A case study of Finland, Japan, and India. Teoksessa A. Kallioniemi (toim.), Uudistuva ja kehittyvä ainedidaktiikka. *Ainedidaktinen symposium*, 8(2008), 783-796.
- Qiang, K. (2013). Paralanguage. *Canadian Social Science*, 9(6), 222-226.
- Singapore Tourism Board. (2022). *STB expects 4 to 6 million international visitor arrivals for 2022 as tourism recovery gains momentum*. <https://stb.gov.sg/stb/en/media-centre/media-releases/STB-expects-4-to-6-million-international-visitor-arrivals-for-2022-as-tourism-recovery-gains-momentum.html>
- Singapore Tourism Board. (2020). *Tourism Statistics*. <https://stan.stb.gov.sg/content/stan/en/tourism-statistics.html>
- SingStat. (2022). *Population*. <https://singstat.gov.sg/modules/infographics/population>
- Stromwall, L. A., Granhag, P. A., & Hartwig, M. (2004). Practitioners' beliefs about deception. In Granhag, P. A., & Stromwall, L. A., (Eds.), *The Detection of Deception in Forensic Contexts* (pp. 15-40). Cambridge: Cambridge University Press.
- Taylor, P., Larner, S., Conchie, S., & Van der Zee, S. (2014). Cross-cultural deception detection. In P. A. Granhag, A. Vrij, & B. Verschuere (Eds.), *Deception Detection: Current Challenges and Cognitive Approaches*. (pp. 175-202). Chichester: Wiley Blackwell.
- Tsai, J., L., Levenson, R., & McCoy, K. (2006). Cultural and temperamental variation in emotional response. *Emotion*, 6(3), 484-497. Doi: 10.1037/1528-3542.6.3.484
- Ulijin, J. M., & St Amant, K. (2000). Mutual intercultural perception: How does it affect technical communication? Some data from China, the Netherlands, Germany, France and Italy. *Technical Communication*, 47(2), 220-237.

Waiflein, M. (2013). *The progression of the field of kinesics*. Senior Theses Anthropology, 3. Illinois State University. <https://ir.library.illinoisstate.edu/sta/3/>

Warren, G., Schertler, E., & Bull, P. (2009). Detecting deception from emotional and unemotional cues. *Journal of Nonverbal Behavior*, 33(1), 59-69.

Wan, W. (2021). Integrating locals and foreigners in a multicultural workplace. *Singapore Institute of Management*. <https://m360.sim.edu.sg/article/pages/integrating-locals-and-foreigners-in-a-multicultural-workplace.aspx>

Zloteanu, M., Bull, P., Krumhuber, E. G., & Richardson, D. C. (2021). Veracity judgement, not accuracy: Reconsidering the role of facial expressions, empathy, and emotion recognition training on deception detection. *Quarterly Journal of Experimental Psychology*, 74(5), 910-927.

RECENT PUBLICATIONS BY HOME TEAM STAFF

BOOKS

A Woman's Journey Home – Stories of Hope & Empowerment

By Charlotte Stephen, Camelia Liow, Marilyn Lee, Lowshanthini Panesilvam and Isabel Tan

Co-published by Singapore Prison Service and Singapore Anti-Narcotics Association, September 2022, 125 pages

The stories in this book are by 16 former women drug users who have shared a part of their life that was difficult, painful but also joyful and triumphant. These women share their experiences of victimisation and trauma which was a significant part of their life leading up to their offending behaviours. They have also spent time detained in a Drug Rehabilitation Centre as well as at Changi Women's Prison. The narratives shared and the gendered perspective provided in the book trace the path of women offenders into the justice system and their journey towards change and long-term recovery. The book hopes to fill the gap in the knowledge of women's experiences in committing offences and highlights the oversight of understanding in this area.

Camelia Liow and Marilyn Lee are with the Singapore Prison Service. Charlotte Stephen and Isabel Tan are with the Singapore Anti-Narcotics Association (SANA). Lowshanthini Panesilvam was formerly with SANA.



JOURNAL ARTICLES

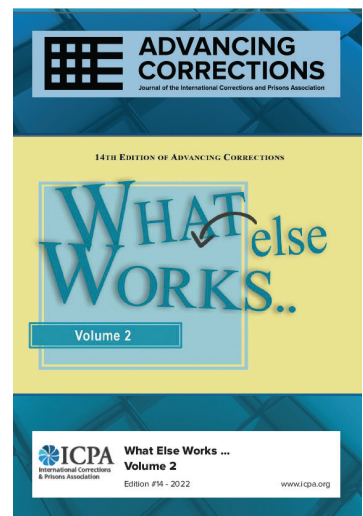
Empathy – Building Communities of Support in the Singapore Prison Service

By Chua Yi Gang and Chan Sook Wei

In *Advancing Corrections Journal*, Edition Number 14, Volume 2 International Corrections & Prisons Association, October 2022

This paper aims to share the conception and implementation of the Empathy Programme (ETP), a ground-up initiative by the Singapore Prison Service (SPS). ETP is a collaborative group process that uses principles from Restorative Practice to promote and foster the objectives of Accountability and Responsibility, Contrition, Empathy, and Sense of Community and Rapport among inmate communities. The evaluation examines the impact of ETP, in terms of its outcomes, effectiveness, and the implementation processes. Findings suggest that ETP promotes better relationships with others, development of interpersonal skills and better behavioural management of inmates.

Chua Yi Gang and Chan Sook Wei are with the Singapore Prison Service



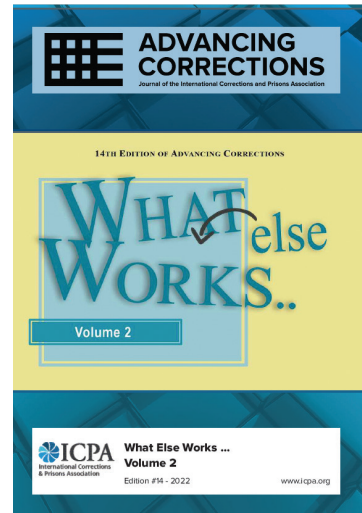
From “Closed” to “Open” groups for sexual offenders in Singapore: Clinical and Operational considerations and preliminary findings

By Paul Zhihao, Yong; Arvina Manoo and Kwek Boon Siang

In *Advancing Corrections Journal*, Edition Number 14, Volume 2
International Corrections & Prisons Association, October 2022

In 2019, the Singapore Prison Service converted a sexual offender rehabilitation programme from a closed group to an open group format after facing limitations with the former. In this paper, we describe the programme, discuss clinical and operational considerations for the conversion, and shared our preliminary findings. We illustrate how an open group – when operationalised based on sound clinical and operational considerations – is preferred over a closed group for sexual offenders in Singapore’s prison context.

Paul Yong, Arvina Manoo and Kwek Boon Siang are with the Singapore Prison Service.



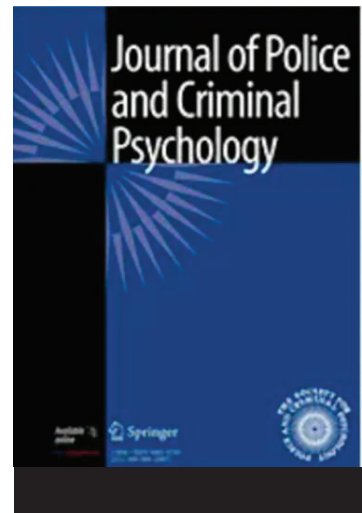
Understanding the Workload of Police Investigators: a Human Factors Approach

By Yong Sheng Tan, Alyah Dinah Zalzuli, Jansen Ang, Hui Fen Ho and Cheryl Tan

In *Journal of Police and Criminal Psychology*, 37:447–456
Springer Link, 24 March 2022

Criminal investigative work entails a diverse array of tasks and responsibilities, ranging from interviewing suspects and victims to managing the paperwork and necessary follow-ups for each case. The present study sought to evaluate the workload and workload impacts of police investigators in a metropolitan police agency. The NASA-Task Load Index (NASA-TLX), a well-established human factor measure of workload, was administered on 759 investigators as a quantitative measure of workload. Subsequently, 49 investigators participated in focus group discussions to provide deeper insight into their workload experiences. The results indicate that police investigators reported a markedly high level of workload when compared to similar human factor studies in the literature. Findings of the focus group discussions attributed the perceived high workload to various contributors such as operational challenges, dealing with the public and external agencies, as well as organisational challenges. Interventions to manage the heavy workload were discussed. The human factors approach can be a suggested approach to understand the task load of police officers.

Alyah Dinah Zalzuli, Jansen Ang, Hui Fen Ho, and Cheryl Tan are with the Singapore Police Force. Yong Sheng Tan was previously with the Singapore Police Force.



"Take a Break!": A Qualitative Study of Shift-Duty Police Officers' On-The-Job Breaks

By Shi Min Toh and Eunae Cho

In *Police Quarterly*, Volume 0(0), pages 1 to 27
SAGE Publications, 2022

Criminal investigative work entails a diverse array of tasks and responsibilities, ranging from interviewing suspects and victims to managing the paperwork and necessary follow-ups for each case. The present study sought to evaluate the workload and workload impacts of police investigators in a metropolitan police agency. The NASA-Task Load Index (NASA-TLX), a well-established human factor measure of workload, was administered on 759 investigators as a quantitative measure of workload. Subsequently, 49 investigators participated in focus group discussions to provide deeper insight into their workload experiences. The results indicate that police investigators reported a markedly high level of workload when compared to similar human factor studies in the literature. Findings of the focus group discussions attributed the perceived high workload to various contributors such as operational challenges, dealing with the public and external agencies, as well as organisational challenges. Interventions to manage the heavy workload were discussed. The human factors approach can be a suggested approach to understand the task load of police officers.

Shi Min Toh is with the Singapore Civil Defence Force, and was previously from the Singapore Police Force. Eunae Cho was previously with the Nanyang Technological University, Singapore.





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.

HOME TEAM ACADEMY



A LEADING CORPORATE UNIVERSITY IN HOMEFRONT SAFETY & SECURITY

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